VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

DIPLOMOVÁ PRÁCE

Brno, 2017 Bc. Ondřej Vala

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ
DEPARTMENT OF TELECOMMUNICATIONS

ANALÝZA SMĚROVACÍCH PROTOKOLŮ POUŽÍVANÝCH V MANET SÍTÍCH
ANALYSIS OF ROUTING PROTOCOLS USED IN MANET NETWORKS

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE
AUTHOR
Bc. Ondřej Vala

VEDOUCÍ PRÁCE
SUPERVISOR
Ing. Anna Kubánková, Ph.D.

BRNO 2017

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Diplomová práce

magisterský navazující studijní obor **Telekomunikační a informační technika**
Ústav telekomunikací

Student: Bc. Ondřej Vala ***ID:*** 120807
Ročník: 2 ***Akademický rok:*** 2016/17

NÁZEV TÉMATU:

Analýza směrovacích protokolů používaných v MANET sítích

POKYNY PRO VYPRACOVÁNÍ:

Nastudujte principy sítí MANET a směrovací protokoly používané v těchto sítích. Zaměřte se na protokoly OLSR, AODV and HWMP. Seznamte se s prostředím NS-3 pro simulaci bezdrátových sítí. V NS-3 vytvořte model MANET sítě standardu 802.11n a několik scénářů pro pohyb stanic. Simulujte přenos v síti a použití různých směrovacích protokolů pro každý scénář. Analyzujte kvalitativní parametry přenosu při použití různých směrovacích protokolů.

DOPORUČENÁ LITERATURA:

[1] Daniil Meitis, Danil Vasiliev, Albert Abilov. Simulation of MANETs routing protocols for UAVs. Proceedings Fourth Forum of Young Researchers. Izhevsk, Publishing House of Kalashnikov ISTU, pp. 358-363, 2014.

[2] ns-3. [online]. [cit. 2016-09-13]. Dostupné z: https://www.nsnam.org/

Termín zadání: 1.2.2017 ***Termín odevzdání:*** 24.5.2017

Vedoucí práce: Ing. Anna Kubánková, Ph.D.
Konzultant:

doc. Ing. Jiří Mišurec, CSc.
předseda oborové rady

ABSTRAKT

Tato diplomová práce se zabývá analýzou směrovacích protokolů používaných v MANET sítích se zaměřením na protokoly OLSR, AODV a HWMP. Práce se skládá z teoretické části, kde jsou popsány směrovací protokoly, které se používají v MANET sítích a jejich aplikování v sítích FANET. V praktické části práce jsou rozebrány vytvořené modely mobility, které jsou použity pro porovnání směrovacích protokolů pomoci vytvořených scénářů mobility podle kvalitativních parametrů sítě.

KLÍČOVÁ SLOVA

MANET, FANET OLSR, AODV, HWMP, Network Simulator, NS-3, směrování, Ah-Hoc

ABSTRACT

This diploma thesis is analysis of routing protocols used in MANET networks focusing on protocols OLSR, AODV and HWMP. The work consists of a theoretical and practical part. The theoretical part describes the routing protokols, which are used in MANET networks and their applications to FANET networks. In practical part, there are describes of created mobility model in the NS-3, which are used for comparison routing protocols on the created scenarios of mobility according to the qualitative parameters of the networks.

KEYWORDS

MANET, FANET, OLSR, AODV, HWMP, Network Simulator, NS-3, routing, Ah-Hoc

VALA, Ondřej *Analýza směrovacích protokolů používaných v MANET sítích*: diplomová práce. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2017. 55 s. Vedoucí práce byl Ing. Anna Kubánková, Ph.D.

PROHLÁŠENÍ

Prohlašuji, že svou diplomovou práci na téma „Analýza směrovacích protokolů používaných v MANET sítích“ jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené diplomové práce dále prohlašuji, že v souvislosti s vytvořením této diplomové práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

Brno ....

(podpis autora)

PODĚKOVÁNÍ

Rád bych poděkoval vedoucímu diplomové práce paní Ing. Anně Kubánkové, Ph.D. za odborné vedení, konzultace, trpělivost a podnětné návrhy k práci.

Brno ....

(podpis autora)

OBSAH

SEZNAM OBRÁZKŮ

ÚVOD

Cílem této práce bylo popsat a analyzovat směrovací protokoly, které se používají v sítích typu MANET. Konkrétně se jedná o protokoly Optimized Link State Routing Protokol (OLSR), Ad hoc On-Demand Distance Vector Routing Protocol (AODV) a Hybrid Wireless Mesh Protocol (HWMP).

V úvodních kapitole této práce jsou popsány teoretické základy sítě typu Mobile ad hoc network (MANET) a následně popsány výše uvedené protokoly. Následující kapitoly posloupně popisují praktickou část této diplomové práce v programu Network Simulátor 3, kde je jen krátce charakterizován tento simulační program, ovšem důkladněji se tento text věnuje popisu vzniku scénářů mobility, které budou sloužit pro analýzu směrovacích protokolů v diplomové práci se známými parametry pohybu. Díky znalosti těchto parametrů lze jednoduše demonstrovat výhody a nevýhody výše uvedených směrovacích protokolů při extrémních podmínkách pohybu síťových prvků ve vysokých rychlostech. V této práci se jedná konkrétně o síť typu Flying Ad-Hoc Wireleess Networks (FANET), tedy zařízení schopné letu. V poslední kapitole 3 jsou popsány vytvořené modely mobility. Na tyto modely byly aplikovány směrovací protokoly a porovnány a analyzovány se stejnými vstupními parametry simulace za pomocí kvalitativních parametrů sítě, které jsou zaneseny v grafických závislostech na čase.

1 SÍTĚ TYPU MANET

V této úvodní kapitole je popsána charakteristika sítě typu MANET, celým názvem „Mobile Ad hoc Networks“. Jedná se o decentralizovaný bezdrátový typ sítě, který nezávisí na existující infrastruktuře, jako jsou směrovače v pevných sítích, nebo přístupové body v sítích bezdrátových, ale na rovnocenných uzlech, které komunikují ve volné topologii mezi sebou. Tato technologie nachází uplatnění jak ve vojenském odvětví, tak i v odvětví soukromém, kde může suplovat drahou technologii buňkového typu, nebo tuto technologii vylepšovat.

Vize MANET sítě je vytvářet stabilnější a účinější bezdrátový provoz v mobilních bezdrátových sítích se začleněním směrovacích funkcí do mobilního uzlu. Ty mobilní sítě mají dynamickou rychle se měnící topologii, kde náhodně přibývají, nebo ubývají síťové prvky, které pracují s omezenou šířkou pásma. MANET sítě mohou pracovat jak v autonomním režimu, tak i s propojením se síti pevnou.

Uzly v MANET síti jsou vybaveny anténami pro bezdrátové vysílaní a příjímání, které mohou být všesměrové, směrové, případně řiditelné, nebo jejich kombinace.

Sítě typu MANET mají tyto základní charakteristické vlastnosti:

- Dynamická topologie: Uzly se mohou libovolně pohybovat, z čehož vyplývá, že topologie sítě se může náhodně a rychle měnit v nepředvidatelných časech a spojení mohou být koncipována jako jednosměrná, nebo obousměrná spojení.
- Proměnlivá kapacita spojů a omezená šířka pásma: U bezdrátového spojení se předpokládá, že bude mít mnohem menší propustnost, než pevná síť. Ovšem musí se brát na zřetel mnohonásobný přístup Media Access Control (MAC), rušení v prostoru, dostupnost signálu atd. Tím pádem je maximální reálná přenosová rychlost mnohem menší než teoretická.
- Omezený energetický provoz: Jelikož je většina zařízení v MANET sítích napájena z vyčerpávajících se zdrojů, je velmi často takové zařízení navrženo pro maximální úsporu energie.
- Omezená fyzická bezpečnost: Mobilní bezdrátové sítě jsou obecně náchylnější k fyzickým bezpečnostním hrozbám, než jsou pevné kabelové sítě. Existuje zvýšená pravděpodobnost odposlechů, útoků pro odmítnutí služby (DDOS), nebo falšovaní zpráv. Ovšem zde může působit decentralizovaná struktura jako výhoda proti hrozbám oproti klasickým sítím.[1]

1.1 FANET - „Flying Ad-Hoc Networks“

Tato kapitola se blíže věnuje sítím FANET, zejména se zaměřuje na rozdíly mezi sítěmi typu MANET a FANET, které jsou popsány již minulé kapitole 1 FANET

celým jménem „Flying Ad-hoc Networks“ je skupina bezpilotních létajících strojů v anglické literatuře označovány jako „Unmanned Air Vehicle (UAV)“, které nepotřebují pro komunikaci mezi sebou žádné řídicí prvky, které standardně využívají bezdrátových sítích jako jsou: přístupové body, nebo směrovače. Standardně v sítích FANET jeden z prvků musí být připojen k síťovému prvku, který může být na zemi, nebo lze využít satelitní připojení. Ovšem ten slouží jen pro propojení s pevnou sítí, které může sbírat informace od UAV, nebo UAV mohou tvořit most přes nějakou geografickou překážku, nebo nezasíťovaným územím. Dnešní době tato technologie nabírá na obrátkách, jelikož se už dnes jedná o levnou technologii. Tato technické řešení začíná nacházet cestu hlavně ve vojenském i v civilním prostředí.

Hlavni rozdíly mezi FANET a MANET resp. VANET sítěmi jsou:

- Stupeň mobility FANET sítí je mnohem vetší než u MANET, nebo VANET „Vehicular Ah-Hoc Network“ uzlů. Klasicky sítí u MANET jsou to chodící lidé, nebo automobily. U FANET se standardně jedná o létající uzly.
- V závislosti na vysoké mobilitě uzlů FANET se topologie mění častěji než topologie typická pro MANET síť
- Stávající sítě ad-hoc mají za cíl vytvořit klient - klient připojení. FANET také potřebuje vytvořit klient - klient síť pro vzájemné propojení pro koordinaci a spolupráci UAV. Kromě tohoto shromažďuje data od jednotlivých UAV k prvků, který je propojen s řídicím střediskem např. přes satelit, nebo s prvkem připojeným k pevné sítí. V důsledku toho musí FANET podporovat komunikaci klient - klient a současně konvergovat část datového toku.
- Typické vzdálenosti mezi FANET síťovými uzly je mnohem vetší než u MANET, nebo VANET. Tím pádem jsou zde odlišné hardwarové komponenty, které budou ovlivňovat kvalitu radiového spojení, jak rušením tak zde může vznikat i situace se skrytým sítovým uzlem.
- Multi-Systémy UAV mohou obsahovat různé typy senzorů a každý druh senzorů mohou požadovat různé strategie dodání dat.

Výše popsáné rozdíly definují sítě typu FANET a oddělují je od ostatní druhů sítí z rodiny ad-hoc. [7] [11] [12]

1.1.1 Parametry FANET

V této kapitole budou popsány základní parametry, které jsou důležité pro sítě typu FANET.

Model mobility

Na rozdíl od sítí typu MANET, kde se standardně jako model pohybu v simulacích používá náhodný směr pohybu po určitém terénu a VANET sítí, kde je pohyb v

simulacích definován jako pohyb po silnicích a dálnicích, kterému nejlépe odpovídá model pohybu mřížkového typu, neboli „Manhattan“, kde pohyb sítových uzlů je velmi dobře predikovatelný, toto ovšem u síťí typu FANET neplatí. Autonomnímu víceprvkovému systému v FANET síťí nelze s jistotou predikovat pohyb protože není dopředu znám, jelikož letový plán se může velmi rychle měnit a pohyb síťových uzlů je velmi rychlý a topologie sítě se rychle mění. Jednou možností mobility je tzn. kruhový pohyb s daným poloměrem kruhu, který je definován ve dvojrozměrném disku.

V článku „Mobility Models for UAV Group Reconnaissance Applications “ z Linköping University ve Švédsku je studie, která definuje pohyb založený na feromonech. V krátkosti se jedná o rozložení UAV na daném prostoru podle feromonů. UAV jsou zdroji feromonů a informace o svém feromonu a oblasti pokrytí jsou sdíleny s daty přenosu. Ostatní UAV vyhledají oblasti kde je co nejmenší výskyt feromonů. Tím dojde k rovnoměrnému zasíťování dané oblasti. Více informací o mobilitě založené na feromonech můžete najít v odkazech na literaturu s číslem [13] [11][12][13].

Změna topologie sítě

Jelikož v sítích FANET, kde UAV dosahují velkých rychlostí a to až do rychlostí 450 km/h je změna topologie častějším jeven. To má za následek několik problémů které se mohou projevovat. Častým jevem může být skrytý síťový uzel, nebo neplatné směrovací údaje ve směrovacích tabulkách. Zde jsou jen okrajově popsány tyto problémy, ovšem podrobněji se tato práce bude zabývat danou problematikou v dalších kapitolách.[11][12]

Model radiového přenosu

Ve většině případů sítě FANET budou pracovat ve vysoké výšce nad úrovni zemi, tím pádem zde oproti jiným typům ad-hoc sítí nebude mít vliv interference signálů s odraženými signály od překážek a geografického terénu. Pro simulace se jeví jako nejvhodnější model nazývány „Free space propagation model“, který je definován jako rovnice:

$$P_r = \frac{P_t G_t G_r \lambda^2}{(4\pi)^2 d^2 L} \tag{1.1}$$

kde:

- P_r - Přijatý výkon v dBm
- P_t - Vysílaný výkon v dBm
- G_t - Vysílací zisk antény v $[dBi]$
- G_r - Přijímací zisk antény v $[dBi]$

- λ - Vlnová délka, která se vypočte ze vztahu $\lambda = \frac{C}{f}$, kde C je rychost světla ve vakuu a f je frekvence např. 5 GHz
- d - Je vzdálenost mezi vysílačem a přijímačem v $[m]$
- L - Ztráta systému v $[-]$ [8][11][14]

Energetická náročnost a životnost sítě

Pro klasické MANET sítě je tento parametr nesmírně důležitý, jelikož malé počítačové zařízení, které je napájeno baterii má omezenou životnost. Tím pádem směrovací protokoly v sítí typu MANET byly navrhovány jako energetický nenáročné, aby celková výdrž na baterii byla co největší. Avšak to není případ pro FANET síť, ta disponuje velkým zdrojem energie a tento problém se zde tedy nevyskytuje, ale nesmíte zapomínat, že FANET může fungovat i na malých UAVs, kde naopak problematika energetická náročnost hraje velkou roli.

Výpočetní výkon síťových uzlů

V koncepci sítě ah-hoc je každý uzel i směrovačem a tím pádem jsou na něho kladeny výpočetní nároky. Obecně v sítích MANET, kde se síť skládá převážně z notebooků, smartphonů a PDA, které disponují omezeným výpočetním výkonem, tak zpracování dat v reálném čase může být problém. V sítích FANET i VANET existují síťové uzly, které disponují velkým výpočetním výkonem a tyto problémy se zpracování dat v reálném čase nemají. Většina UAV má dostatek energie a prostoru pro instalaci výkonného výpočetního prvku. Jediným limitujícím faktorem může být váha, ovšem v dnešní době miniaturizace hardwarů je možné do platforem UAV umístit výkonný výpočetní hardware.

Přizpůsobivost

Během provozu se v sítích typu FANET může měnit několik proměnných, je potřeba aby systém byl velmi rychle adaptovatelný na změny a tím eliminovat výpadky v sítí během přenosu. FANET uzly jsou vysoce mobilní prvky, které vždy mění své umístění, tím pádem topologie sítě bude velmi variabilní a vzdálenosti mezi jednotlivými prvky nebude konstantní a budou se během nasazení měnit. Další faktor musí počítat i s výpadkem jednotlivého uzlu a adaptace na tuto událost. Tedy buď mít redundantní spoje, které tuto událost vykryjí, nebo adaptivní mobilitu, která přeskupí jednotlivé uzly do jiné topologie. Další aspekt je počasí. To se může velice rychle změnit a v radiové prostředí se mohou vytvořit překážky formou mraků, nebo elektrostatického rušení. FANET sítě se mohou setkávat s úmyslným rušením radiové pásma apod. Ze všemi těmito aspekty se musí počítat a při návrhu FANET sítě je zohlednit tak, aby se sama mohla přizpůsobit proti jakýmkoliv změnám, nebo poruchám. Fyzická vrstva by se měla přizpůsobovat hustotě jednotlivých uzlů,

vzdálenosti mezi jednotlivými prvky a změnám prostředí, síť FANET je schopna naskenovat parametry fyzické vrstvy a vybrat nejlepší nastavení fyzické vrstvy.

Škálovatelnost

FANET sítě by měly být velice dobře škálovatelné, kde zvýšení uzlů a jejich korporativní spolupráce musí zvýšit výkonnost sítě. To je hlavní motivace využití víceprvkového systému UAV. Mezi počtem uzlů a výkonností musí být přímá úměra, kde se zvyšujícím se počtem uzlů se zvyšují výkonnostní parametry sítě. To zajisté bude fungovat jen do určitého počtu uzlů v síti, pak dojde nasycení a přidávání dalších uzlů začne být více na škodu, než přínosem.

Odezva

Odezva je jedním z nejdůležitějších parametrů pro všechny druhy sítí a FANET není výjimkou. Požadavky na odezvu u sítí FANET jsou závislé na druhu aplikace. Například pro aplikace v reálném čase, jako je vojenské sledovaní, musí být doručeny s určitým časovým zpozděním. Další kritickou aplikací je detekce kolize UAV. V článku[15] prezentována analýza, která ukazuje, že směrovací protokoly vyvinuté pro sítě MANET nesplňují požadavky na zpozdění v sítích FANET.[1][7][11][12][15]

2 SMĚROVACÍ PROTOKOLY V SÍTI MANET

2.1 Směrovací protokol Optimized Link State Routing Protocol (OLSR)

Směrovací protokol OLSR celým jménem „Optimized Link State Routing Protocol“ je ze skupiny proaktivních protokolů, to znamená, že každý uzel má informace o kompletní a aktuální topologii sítě a informace potřebné pro směrovaní jsou uloženy ve směrovací tabulce, která je pravidelně aktualizována. Tato vlastnost velice ovlivňuje čas potřebný odeslaní datového toku, kdy mohou být data okamžitě odeslána k cíli. Ovšem tento benefit má za následek ukrajovaní z celkové šířky pásma režijní komunikací pro udržení aktuální směrovací tabulky.

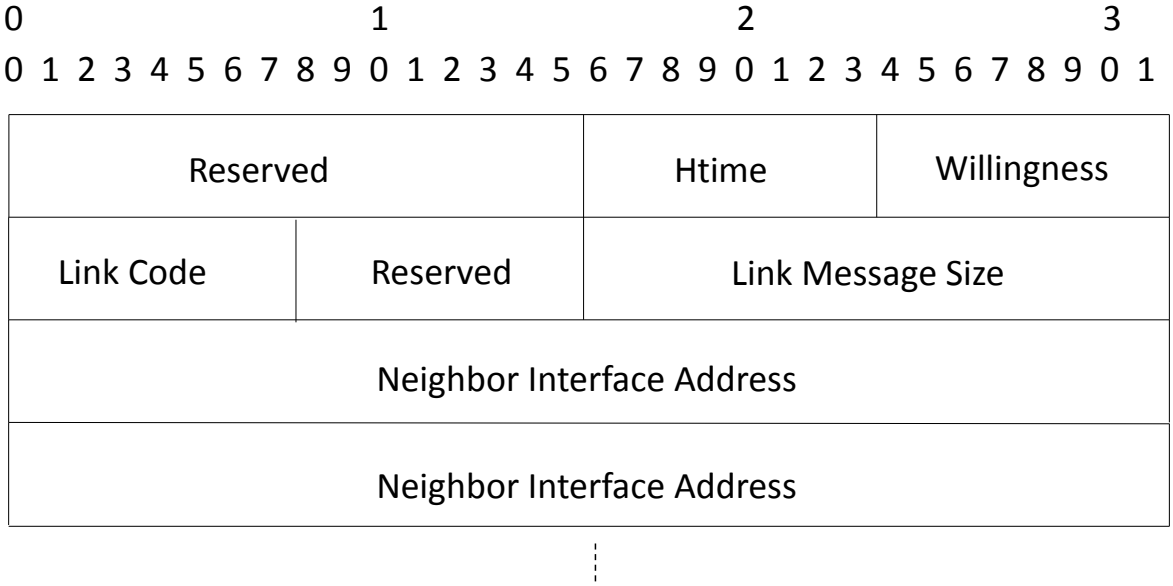
OLSR protokol patří do rodiny „Link-State“ protokolů. Link-state protokoly přestavují pokročilé směrovací protokoly, které na rozdíl od rodiny „distance-vector“ protokolů hledají cestu k cíli ne jen podle počtu přeskoků, ale umí ke každé možné cestě přiřadit váhové koeficienty například podle šířky pásma, zarušení pásma , odezvy, vytížení sousedního uzlu a podobně. A následně pomocí teorie grafů a Dijkstrova algoritmu najít tu nejlepší cestu k cíli.

Pro minimalizaci režie je v protokolu implementována technika MPR (Multipoint relay), kde si každý uzel zvolí několik sousedů, kterým bude rozesílat záplavové zprávy. Protokol zpravidla volí obousměrné spojení, aby se vyhnul ztrátě komunikace a sousedy volí zpravidla podle metriky a počtu skoků a počtu dosažitelných uzlů se vzdálenosti dvou skoků. Tato technika výrazně zjednodušuje výsledný graf sítě pro nalezení nejlepší cesty k cíli. U OLSR protokolu není nevyžadováno aby pro nalezení nejkratší cesty byl cílový uzel připojen mezi vybranými MPR. Ten může být vybrán jiným uzlem než svým MPR. Princip MPR techniky spočívá v tom, že pokud uzel chce odeslat zprávu, zašle záplavovou zprávu na své MPR, ty zase přepošlou zprávu na své MPR a tak to pokračuje dále. Každé MPR si v pravidelně aktualizuje své MPR.

Jak už bylo zmíněno jedná se o proaktivní protokol, pro udržení aktuální znalosti topologie sítě se využívají tzn. HELLO pakety. Ty jsou rozesílány s hodnotou Time to Live (TTL) dvě, která udává dobu života pro dva přeskoky. Pro přenos HELLO zpráv se využívají UDP datagramy, které jsou vysílány jako broadcastové, nebo multicastové zprávy. Z těchto zpráv jsou zjištěni přímí sousedi a případně sousedi sousedů a jejich parametry linky jako jsou kvalita spojení a stav spoje. Tyto parametry poslouží pro volbu MPR uzlů, za splnění výše popsaných podmínek pro zvolení MPR uzlů.

2.1.1 Struktura HELLO zprávy v OLSR

Hello pakety obsahují následující informace, které se využívají pro zjištění aktuální topologie a volbu MPR uzlů. Na obrázku 2.1 je vyobrazena struktura HELLO paketu a jsou zde popsány jednotlivé pole v paketu.



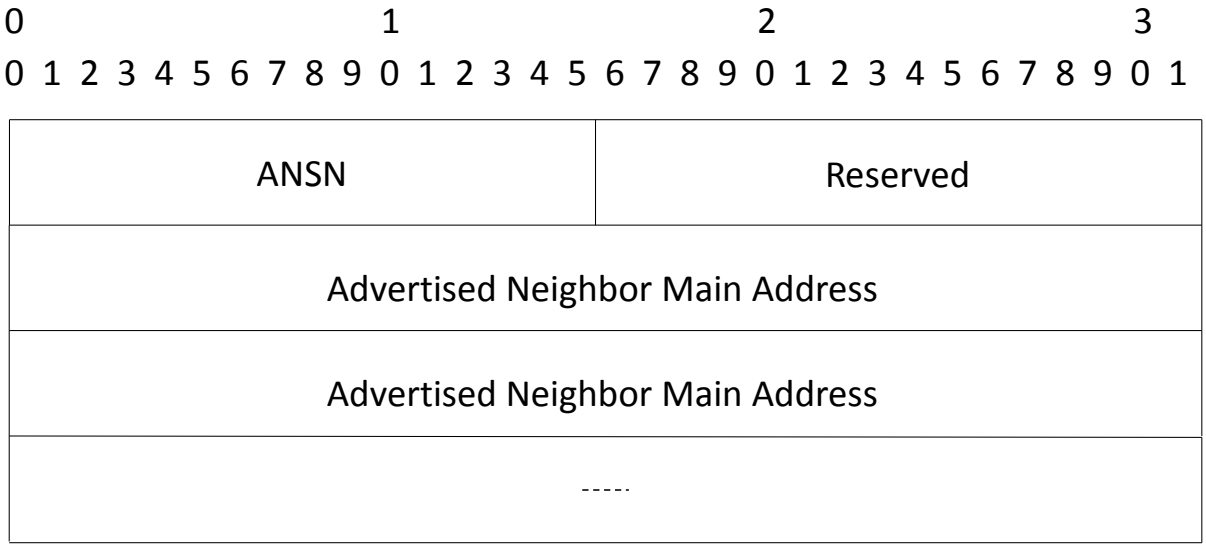
Obr. 2.1: Hello paket protokolu OLSR, převzato a překresleno z [3]

- Reserved: Rezerva pro budoucí použití, dnes vyplněno nulami.
- HTime: Udává časový údaj, jak často zasílat HELLO zprávy. Možné využití pro zjištění kvality spojů a přesnější stanovení metriky.
- Willingness: Ochota komunikace, může nabývat hodnot od 0 do 7, kde nula znamená WILL_NEVER, což znamená, že se uzel s touto hodnotou nikdy nestane MPR. Základní nastavení je hodnota 3, což odpovídá WILL_DEFAULT. Ideální pro volbu MPR je hodnota 7 (WILL_ALLWAYS) poté musí být zvolen jako MPR uzel. Hodnota v poli „Willingness“ se může v průběhu měnit podle různých parametrů jako je vytíženi CPU, stav baterie, viditelnost sousedů atd.
- Link Code: Linkový kód specifikuje informace o lince mezi odesílatelem a sousedním uzlem. Taktéž informuje o stavu linky.
- Link Message Size: Uvadá velikost HELLO zprávy v bajtech od pole „Link Code“ po znova se vyskytující se blok „Link Code“.
- Neighbor Interface Address: Obsahuje adresu sousedů do hodnoty TTL = 2. [3] [4]

2.1.2 Struktura Topology Control (TC) zprávy

Aktuální informace o topologii jsou rozesílány pomocí TC zpráv, kde každý uzel získá přehled na celkové topologii. Tyto adresy rozesílá pouze MPR, ty obsahují adresu zdroje TC zprávy a adresy uzlů. Ostatní adresy mimo MPR nesmí tyto zprávy přeposílat z důvodu možného zahlcení sítě. I zde pro úplnost je uveden formát TC zprávy na Obr.2.2 a popsána jednotlivá pole.

- ANSN (Advertised Neighbor Sequence Number): Sekvenční číslo TC zprávy, pokaždé když uzel detekuje změnu u svých sousedů, inkrementuje toto číslo o jedničku. Uzly pracují pouze se TC zprávami, které obsahují nejvyšší číslo a tímto je zaručena aktuálnost topologie.
- Reserved: Rezerva
- Advertised Neighbor Main Address: Zde jsou uvedeny všechny adresy sousedních uzlů. [3] [4]

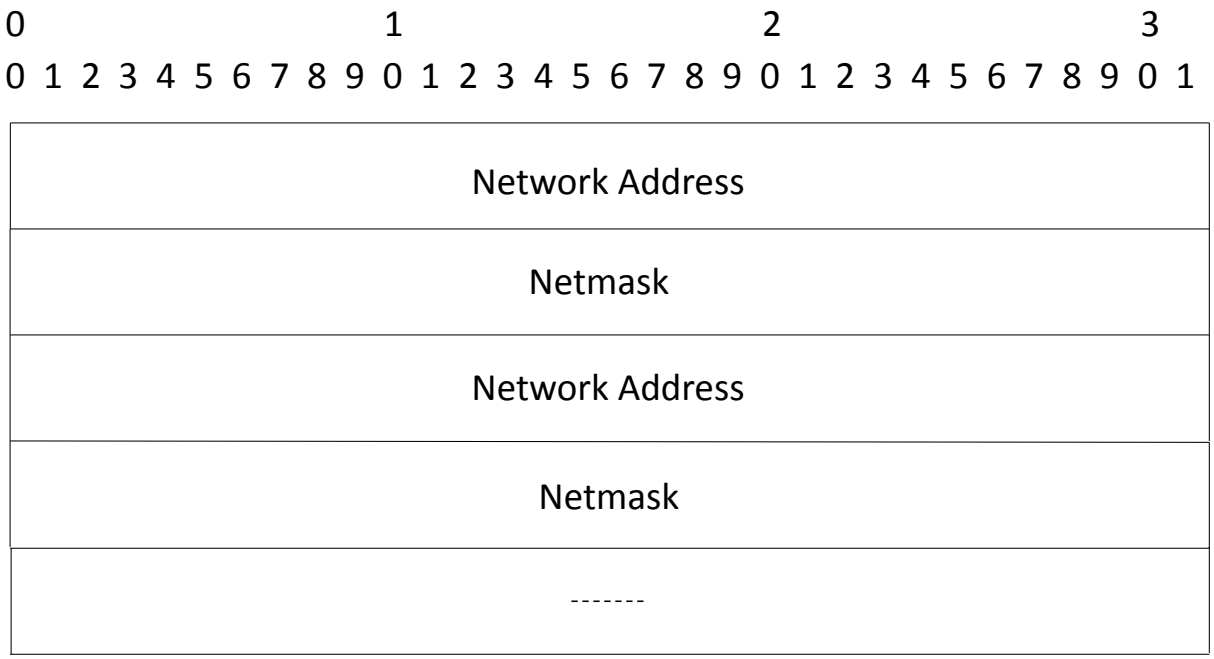


Obr. 2.2: TC paket protokolu OLSR, převzato a překresleno z [3]

2.1.3 Struktura HNA zprávy v OLSR

HNA celým názvem Host and Network Association, jak už z názvu zprávy vyplývá jedná o druh zpráv, které slouží k propojení do sítě, kde protokol OLSR není aplikovaný např. pevná síť. Velmi často je mnoho zařízení připojeno k více sítím najednou a pomocí HNA zpráv lze šířit informace o výchozích branách, kterými tato zařízení disponují. Pod tímto textem je znázorněna struktura HNA zprávy na Obr.2.3 a popsány jednotlivé pole zprávy.

- Network Address: Adresa přidružené sítě.



Obr. 2.3: HNA zpráva protokolu OLSR, převzato a překresleno z [3]

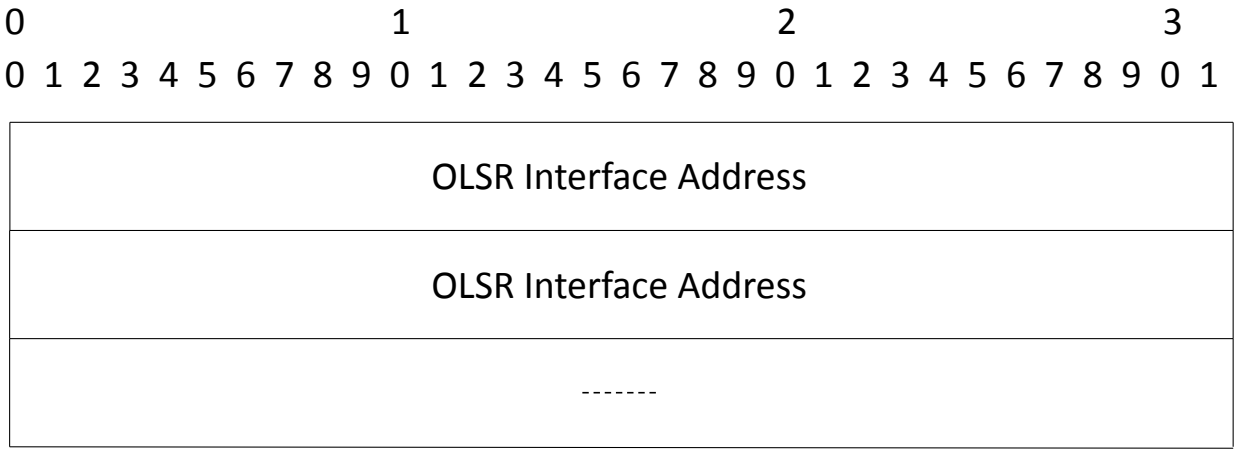
- Netmask: Maska sítě přidružené sítě. [3][4]

2.1.4 Struktura MID zprávy v OLSR

MID (Multiple Interface Declararion) - tento druh zprávy se využívá pokud má zařízení více než jedno komunikační zařízení, které je připojeno k síti přes protokol OLSR. Každý uzel, který disponuje větším množstvím komunikačních zařízení, pravidelně informuje ostatní uzly v síti pomocí MID zprávy. Tyto údaje se promítnou ve směrovacích tabulkách ostatních uzlů v síti. Pro přehlednost je popsána struktura a jednotlivé pole zprávy z Obr.2.4

2.1.5 Formát paketu OLSR

- Packet Lenght: Délka paketu
- Packet Sequence Number: Sekvenční číslo paketu, které označuje číslo paketu tak, aby bylo možné každý paket jednoznačně rozlišit. Toto číslo je inkrementováno o jedničku pokaždé pro nový paket.
- Message Type : Typ zprávy, která může nabývat od 0 do 255. Ovšem od 0 do 127 jsou striktně definovány dle dokumentace viz RFC 3626 [3] od 128 do 255 lze použít pro uživatelské rozšiřující zprávy.

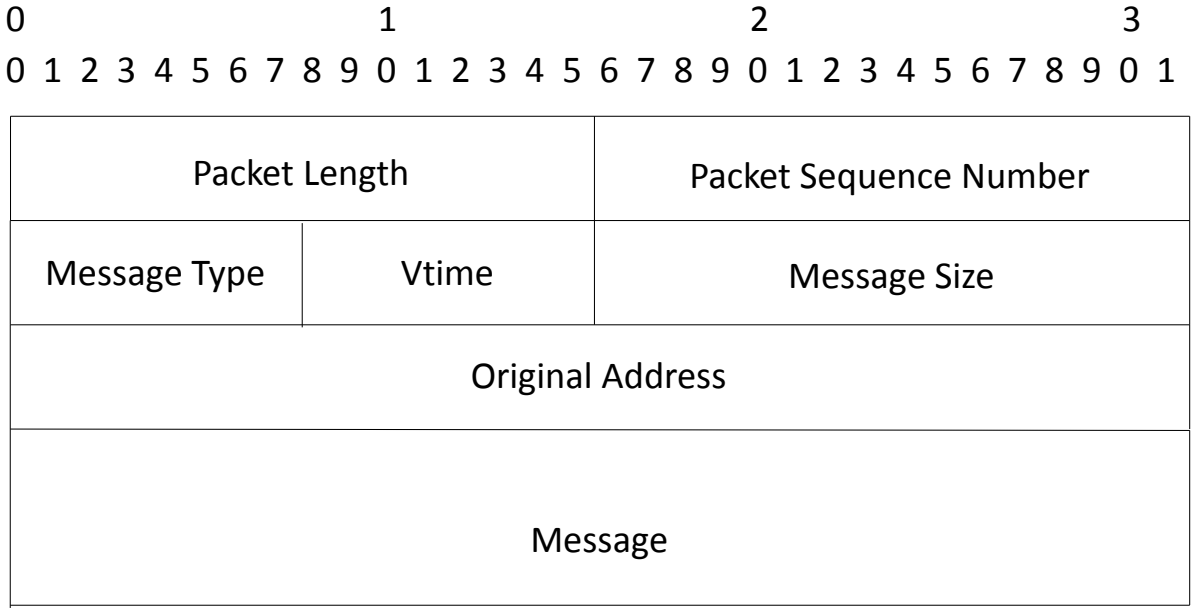


Obr. 2.4: MID zpráva protokolu OLSR, převzato a překresleno z [3]

- VTime: Udává časový údaj, jak dlouho může uzel považovat přijaté informace za validní pokud neexistují informace nové.
- Message Size: Velikost zprávy udávaná v bajtech. Součet je brán od zprávy pole Message Type do pole Message type, nebo pokud není součástí následující zpráva, tak po konec paketu.
- Originator Address: IP adresa zdrojového uzlu.
- Time To Live: Hodnota vyznačuje maximální množství přeskoků (dobu života), která je dekrementována o jedničku při každém přeskoku. Pokud se hodnota zmenší na nulu, paket je zahozen.
- Hop Count: Počítadlo přeskoků, po každém přeskoku je hodnota inkrementována o jedničku. Výchozí hodnota je nula.[3][4]

2.2 Směrovací protokol Ad hoc Demand Distance Vector (AODV)

Tento směrovací protokol se řadí do skupiny reaktivních protokolů, kde cesta k cíli je vytvořena až po vytvoření požadavku. Je to rychle se adaptující směrovací protokol v dynamicky se měnící topologii, který je velmi oblíbený pro svou malou energetickou náročnost a malou zatížitelnost sítě. Jedná se o tabulkový směrovací protokol z rodiny protokolů „distance-vector“. Kde ve směrovací tabulce jsou uloženy pouze uzly, které aktivně komunikují. Pro vyhledávaní sousedů je využit jednoduchý mechanismus dotaz - odpověď za pomocí HELLO zprávy. Pro zamezení směrovacích smyček je pro nalezení optimální trasy aplikovaný Bellmanů-Fordův algoritmus. Algoritmus pracuje na podobném principu jako Dijkstrův algoritmus, ovšem ten nedovoluje ohodnotit hrany grafu záporným číslem. Pro rozlišení směrovacích informací



Obr. 2.5: Struktura paketu OLSR, převzato a překresleno z [3]

je každá zpráva značena sekvenčním číslem, které zaručuje, že budou použity aktuální informace. Tedy pokud existují dvě různé cesty k cílovému uzlu, je použita ta, která má vyšší sekvenční číslo.

Skupina distance-vector se vyznačuje níže popsanými vlastnostmi. Pro každý uzel je vypočtena nejlepší cesta k cíli na základě metodiky počtu přeskoků k cíli, kde každý směrovač si vypočte svou „nejlepší“ trasu a informuje o své nejlepší trase své sousedy. Tímto iteračním procesem je zaručeno nalezení optimální trasy k cíli. Tento proces musí velmi rychle konvergovat k správnému výsledku, ať nedochází k přílišné výměně informací mezi uzly a nezahlcují touto informací šířku pásma. V protokolu AODV mají všechny informace získané pomocí zpráv omezenou validitu. Standardně údaje ze směrovací tabulky platí jen po dobu aktivního spojení, po ukončení spojení se začne odpočítávat čas a po uplynutí doby jsou informace ze směrovacích tabulek vymazány. Po opětovném požadavku na zaslání dat např. stejnému příjemci, musí protokol znova pomocí RREQ popsáném v kapitole 2.2.1 vyhledat znova trasu k cíli.

V podkapitolách pod tímto textem budou rozebrány jednotlivé zprávy, které se používají v protokolu AODV, kde u každé zprávy bude popsán účel zprávy a jeho využití [2][9][10]

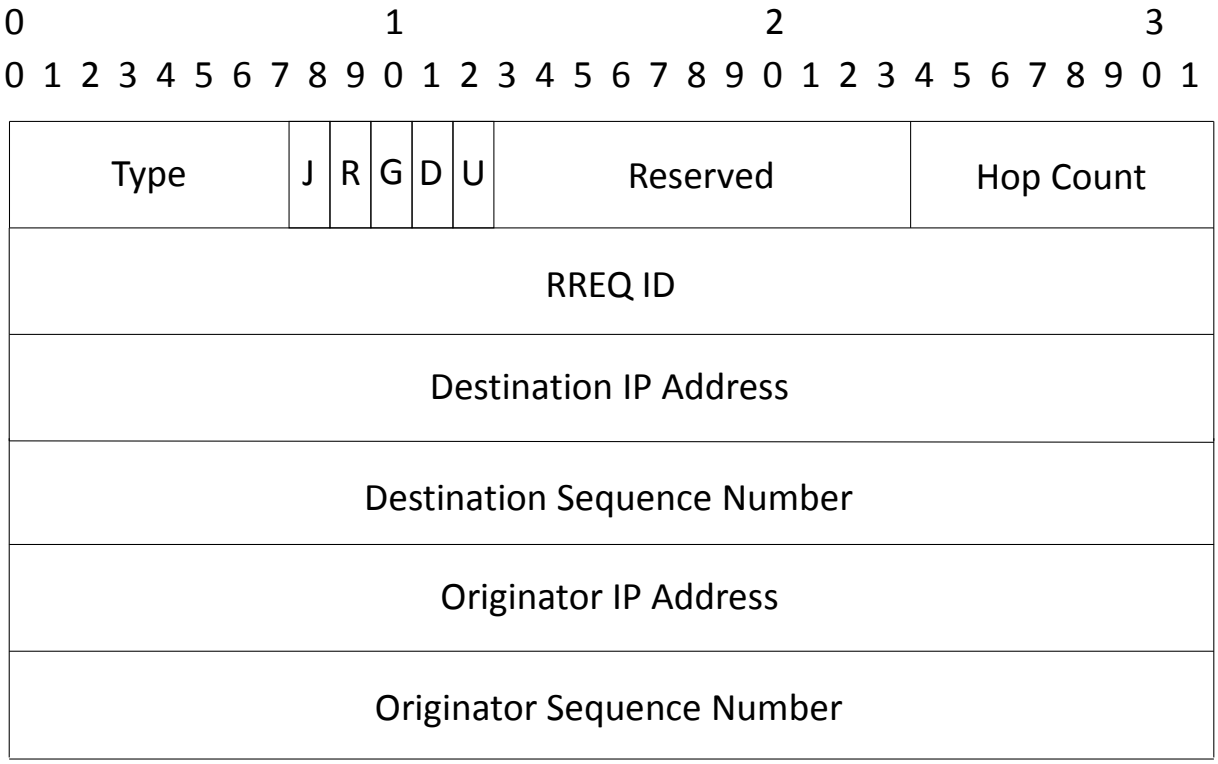
2.2.1 Route Request zpráva AODV

Tato zpráva se využívá pro nalezení trasy k cíli. Zdrojový uzel broadcastově vysílá UDP datagramy se zprávou RREQ (Route Request). Každá stanice v dosahu tento paket přijme, paket aktualizuje jeho informace pro zdrojový uzel a nastaví ve své směrovací tabulce ukazatel zpět na zdrojový uzel. Dále může zprávu přeposlat dále, nebo odpovědět s pomocí zprávy „Route Reply“, která je popsána v kapitole 2.2.2. Pro zamezení přeposílání zprávy, kterou již byla jednou zpracována, jsou všechny zprávy značené unikátním RREQ ID a pokud uzel příjme zprávu se stejným ID, tuto zprávu již dále nepřeposílá a zprávu zahodí ji. Graficky je zpráva znázorněna na Obr.2.6 a níže jsou popsána všechna pole ve zprávě:

- Type: typ zprávy, který je nastaven na hodnotu 1.
- „J“ - Join flag: Příznakový bit pro připojení (rezervováno pro multicast).
- „R“ - Repair flag: Příznakový bit pro opravu (rezervováno pro multicast).
- „G“ - Gratuitous RREP flag: Příznakový bit pro nadbytečnost.
- „D“ - Destination only flag: Příznakový bit zda může cílový příjemce zpráv reagovat na RREQ zprávu.
- „U“ - Unknown sequence number: Příznakový bit, který indikuje, že pořadové číslo není zadáno.
- Reserved: Vyplněno nulou, jeho přijetí je ignorováno.
- Hop Count: Počítadlo skoků od zdroje zprávy k příjemci Route Request zprávy.
- RREQ ID: Unikátní sekvenční číslo, které identifikuje RREQ zprávu, pokud je ve spojení s IP adresou zdrojového uzlu této zprávy.
- Destination IP Address: Cílová IP adresa
- Destination Sequence Number: Poslední sekvenční číslo přijaté v minulosti od zdrojového uzlu zprávy pro jakoukoliv cestu k cíli.
- Originator IP Address: IP adresa zdrojové uzlu této zprávy
- Originator Sequence Number: Aktuální sekvenční číslo, které bylo použito na začátku směrovací trasy ke zdrojovému uzlu žádosti. [2]

2.2.2 Route Reply zpráva (RREP) AODV

Tento typ zprávy je odpovědí na RREQ, kterou mohou odeslat jen ti, kterým žádost RREQ náležela, nebo mají platnou trasu k požadovanému cíli. Jakmile je zpráva Route Reply zasílána zpět ke zdroji zprávy RREQ, jsou na všech uzlech nastavovány ukazatele k požadovanému cíli. Jakmile zdroj požadavku RREQ obdrží zprávu RREP, může okamžitě zasílat data příjemci. Pokud zdroji RREQ dorazí nová zpráva RREP s vyšším pořadovým číslem a obsahuje méně přeskoků, provede aktualizaci své směrovací tabulky. Podrobněji jsou popsána pole této zprávy níže a také graficky znázorněna na Obr.2.7.

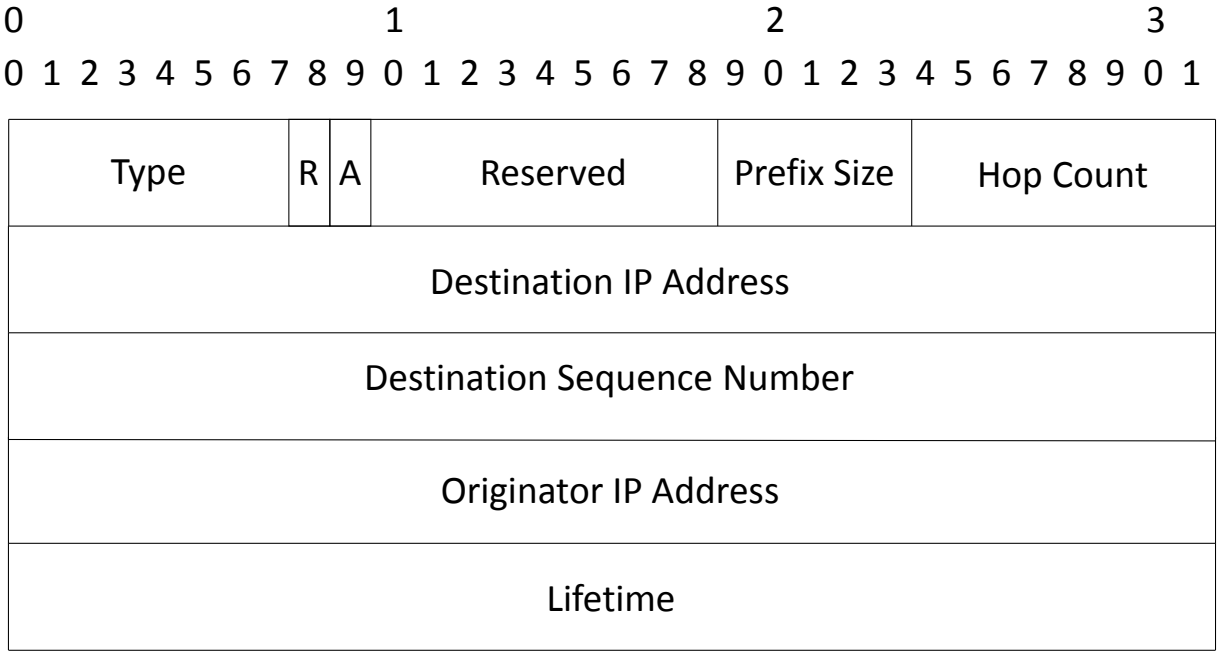


Obr. 2.6: Struktura zprávy Route Request v AODV, převzato a překresleno z [2]

- Type: Typ zprávy, který je nastaven na hodnotu 2.
- „R“ - Repair flag: Příznakový bit pro opravu (použito pro multicast).
- „A“ - Acknowledgment required: Příznakový bit pro požádaní potvrzení.
- Reserved: Vyplněno nulou, jeho přijetí je ignorováno.
- Prefix Size: Pokud není toto pole nulové, určuje tento pětibitový prefix, že pro další skok mohou být použity uzly se stejným směrovacím přefixem.
- Hop Count: počitadlo skoků od zdrojového uzlu k cílovému uzlu.
- Destination IP Address: Cílová IP adresa
- Destination Sequence Number: Zdrojové sekvenční číslo.
- Originator IP Address: IP adresa zdrojové uzlu této zprávy
- Lifetime: Udává čas v milisekundách, jak dlouho je směrovací cesta platná od uzlů, které obdržely RREP zprávu.

2.2.3 Route Error zpráva AODV

V případě chyby v trase k cíli, je vygenerována na posledním funkčním uzlů chybová zpráva, že cílové místo není dostupné je poslána ve směru zdrojového uzlu. Po přijetí chybové zprávy zdrojovým uzlem, jsou posílaná data pozastavena, poté je znova poslána zpráva typu RREQ, zda linka je znova aktivní, nebo zda neexistuje nová



Obr. 2.7: Struktura zprávy Route Reply v AODV, převzato a překresleno z [2]

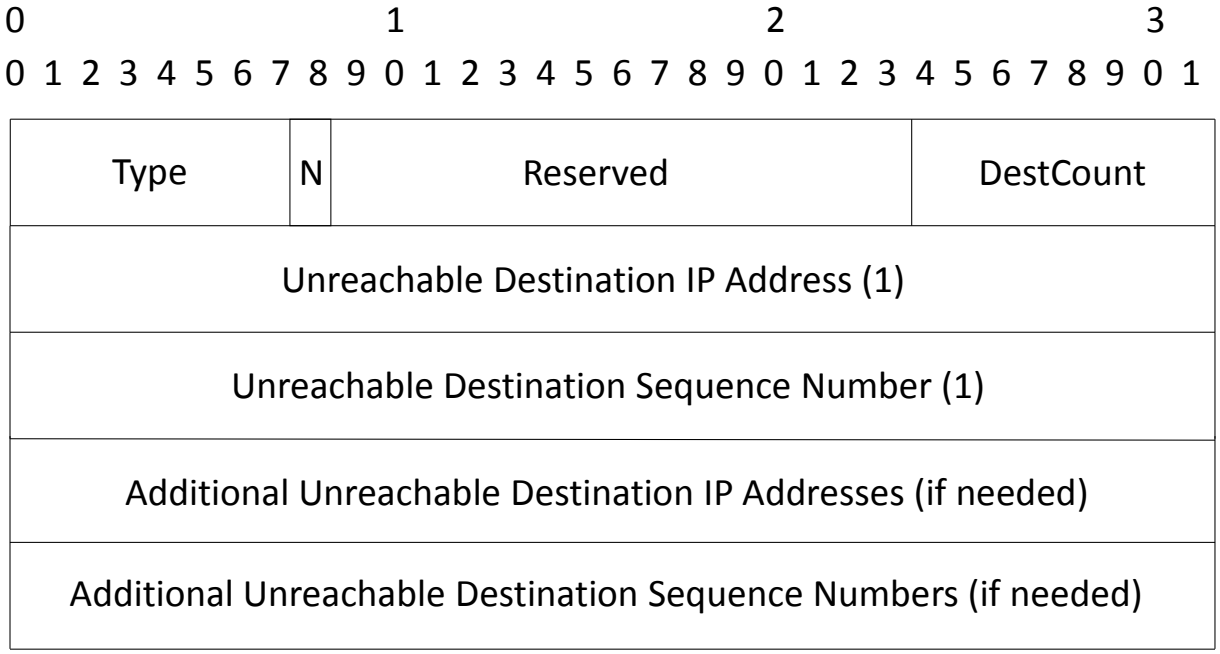
trasa k cíli. I zde jsou popsána jednotlivá pole zprávy RRER a graficky vyobrazena na Obr.2.8.

- Type: Typ zprávy, který je nastaven na hodnotu 3.
- „N“ - No delete flag: Příznakový bit pro nemazání, pokud je nastaven tento příznak, nedojde k smazání trasy k cíli ve směrovací tabulce.
- Reserved: Vyplněno nulou, jeho přijetí je ignorováno.
- DestCount: Počítadlo kolik cílových uzlů je nedostupných, musí být alespoň jeden.
- Unreachable Destination IP Address: IP adresa nedosažitelného uzlu.
- Unreachable Destination Sequence Number:Sekvenční číslo ve směrovací tabulce pro nedosažitelný uzel.

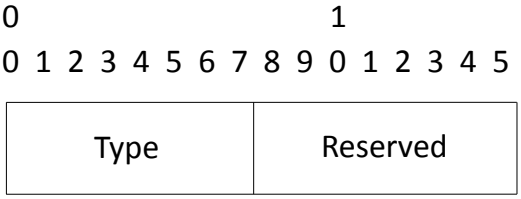
2.2.4 Route Reply Acknowledgmen zpráva AODV

Odpověď na zprávu RREP (Route Reply) pokud byl nastaven příznak „A“, který je popsán v kapitole 2.2.2.

- Type: Typ zprávy, hodnota je nastavena na 4.
- Reserved: Rezerva.



Obr. 2.8: Struktura zprávy Route Error v AODV, převzato a překresleno z [2]



Obr. 2.9: Struktura zprávy v AODV, převzato a překresleno z [2]

2.3 Směrovací protokol Hybrid Wireless Mesh Protocol (HWMP)

Protokol HWMP je kombinací proaktivních a reaktivních protokolů a nazývá se hybridním protokolem. Kombinuje flexibilitu z reaktivních protokolů a znalost topologie z proaktivních protokolů. HWMP protokol přebírá zprávy od reaktivního protokolu AODV, který je popsán v kapitole 2.2 a adaptuje na druhé vrstvě ISO-OSI znalost topologie a přikazovaní metriky uzlům a spojům.

HWMP protokol podporuje dva režimy konfigurace. První režim je (On demand mode) na požádaní, tento mód povoluje MESH protokol pro komunikaci. Tento mód se používá v situaci, kde není známa kostra stromu, ovšem může být použít tento režim i případě kdy kostra stromu topologie již existuje. Druhý režim je povo-

len proaktivní vytváření stromu. V aktivní vyhledávaní se používají zprávy RREQ, který znám z AODV a popsán v kapitole 2.2.1, nebo je použit RANN mechanismus. Jak režim na vyžádání, nebo proaktivní režim. Zmíněné režimy nejsou výhradní a mohou pracovat souběžně. Zprávy které jsou využívány v HWMP jsou RREG, RREP, RRER, které známé z protokolu AODV a jsou popsány v kapitole 2.2 a nový typ zprávy Root Announcement (RANN), která bude popsána níž v této kapitole. HWMP protokol využívá sekvenčních čísel pro rozlišení všech kontrolních zpráv, stejně jako v protokolu AODV, které slouží pro eliminaci smyček ve směrovacích tabulkách a rozlišení novějších zpráv od starších právě pomocí sekvenčního čísla. [2][6]

2.3.1 Režim směrování na požádání (On Demand)

Když zdrojový uzel potřebuje najít trasu v režimu na vyžádaní, vygeneruje zprávu typu RREQ a přes všesměrové vysílání ji odešle. Princip hledání cesty je přebrán z protokolu AODV, který je popsán v kapitole 2.2 a zde znova nebude popisován.

2.3.2 Režim proaktivní vytváření stromu

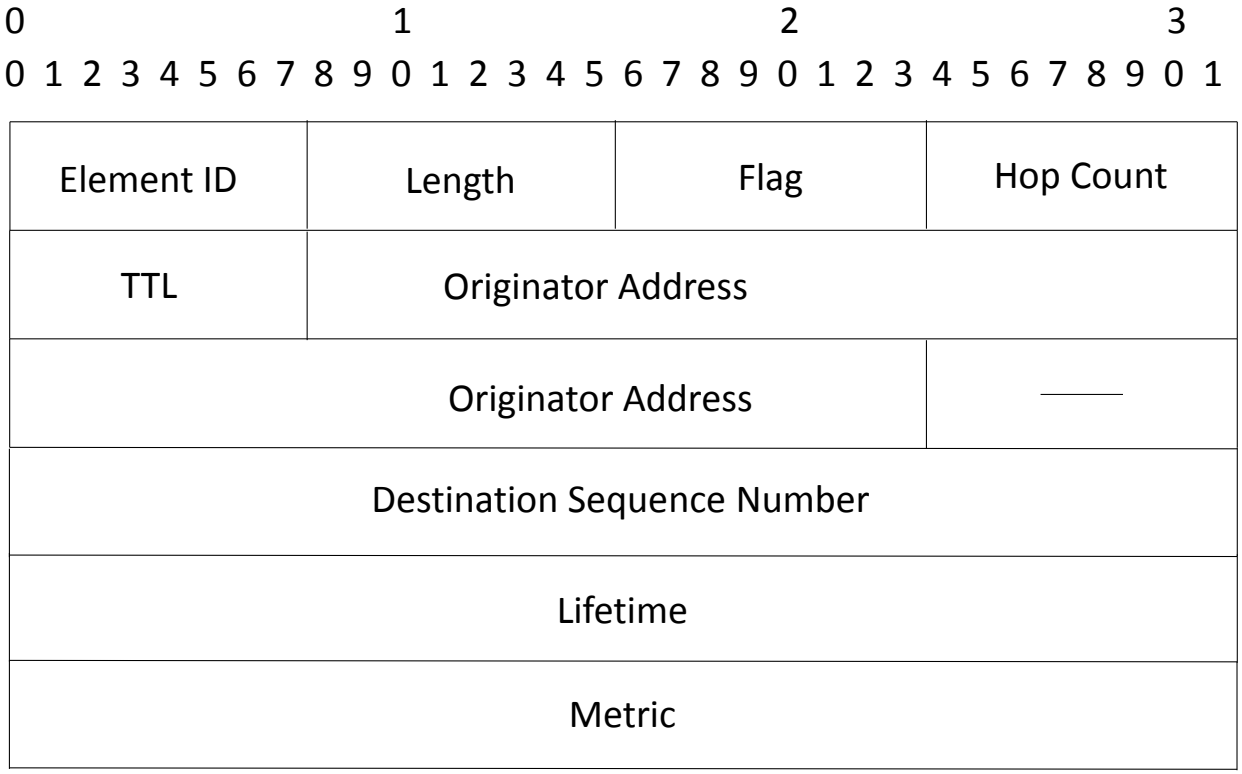
Existují dvě možnosti jak proaktivní režim může fungovat. První je využití RREG známý z AODV, který ovšem pracuje v modu proaktivním. Druhá možnost je použít Strukturu zprávy Root Annoucement (RANN) kterou popisuje Obr.2.10, ty se v periodicky zasílají pro zajištění aktuální směrovací tabulky.

Proaktivní režim s použitím RANN

Kořenový uzel periodicky rozesílá zprávy RANN do sítě. Informace ze zprávy RANN slouží pro vytvoření metriky ke kořenu stromu. Každý uzel, který obdrží zprávu RANN a aktualizuje cestu ke kořenu stromu, zašle unicastovou zprávu RREQ kořenu stromu od něhož zprávu obdržel. Kořen stromu poté odešle každému uzlu zprávu RREP 2.2.2 od něhož obdržel zprávu RREQ 2.2.1. Pomocí RREQ se vytvoří reverzní směrovací cesta od kořene stromu ke zdroji MP. RREP vytvoří dopřednou směrovací cestu od MP ke kořenu stromu.

- ID: ID zprávy RANN
- Length: Délka zprávy RANN
- Flag: Nultý bit rozlišuje zda se jedná o portálovou nebo neportálovou zprávu
- Hop Count: počítadlo skoků
- „TTL“ - Time to Live: Doba života zprávy, která se dekrementuje po každém skoku.
- Originator Address: Adresa původce zprávy.

- Destination Sequence Number: Sekvenční číslo, které specifikuje kořenový uzel stromu.
- Lifetime: Doba validnosti dat zprávy RANN.
- Metric: Vypočtená metrika od původce zprávy k MP.



Obr. 2.10: Struktura zprávy RANN v HWMP, převzato a překresleno z [6]

3 REALIZACE SCÉNÁŘŮ V PROGRAMU NS-3

Tato kapitola se věnuje praktické části diplomové práce, v niž se ověřují teoretické předpoklady směrovacích protokolů, které byly popsány v kapitolách 1 a 2. K realizaci ověření teoretických předpokladů byl vybrán software Network Simulator 3 ve verzi 3.26, kde lze simulovat a analyzovat reálné chovaní síťových prvků a to včetně mobility, na kterých jsou sítě typu FANET založeny.

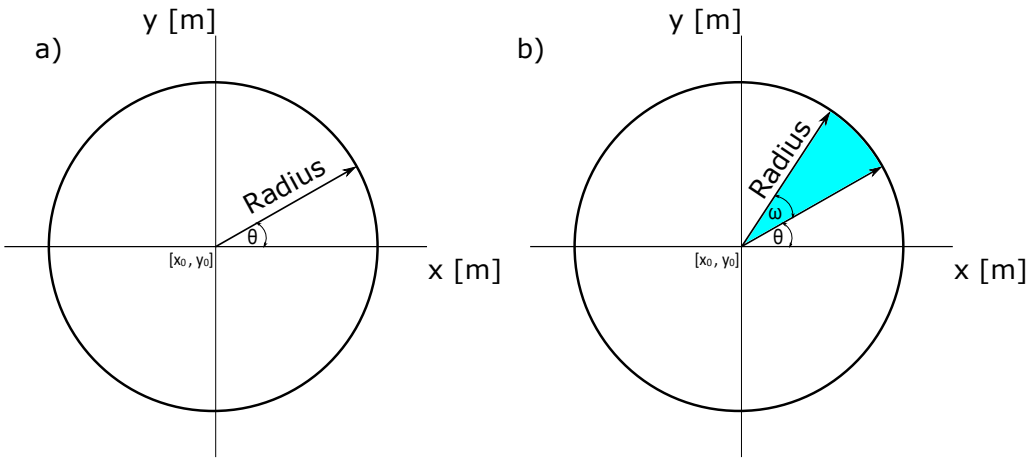
Cílem diplomové práce bylo vytvořit několik scénářů, které budou demonstrovat pohyb mobilních stanic s předem známými parametry, které tak budou zaručovat reprodukovatelnost, ale ovšem i určitou míru nahoditelnosti, která lépe přibližuje chování mobilních stanic v reálném životě. Konkrétněji se jedná o létající UAV, které se pohybují po určité trajektorii s konstantní rychlostí a pro komunikaci využívají standart 802.11n v pásmu 5 GHz. Tyto scénáře budou sloužit pro porovnání sledovaných parametrů mezi různými směrovacími protokoly, které se využívají v sítích typu MANET. Sledované parametry budou podrobněji rozebrány níže v této kapitole.

UAVs se vesměs ve všech scénářích pohybují po kruhovité trajektorii podle zadaného rádiusu s konstantní rychlostí. Tyto UAV jsou rozmístěny do 2D prostoru dle požadovaného scénáře. Jak už bylo zmíněno v odstavci výše je v každém scénáři zaručena i určitá míra náhodného chování a to pomoci uhlů θ. Úhel θ udává v jakém místě se bude UAV v simulaci v čase nula vyskytovat na kruhovité trajektorii. Inicializační hodnota *Theta* muže nabývat hodnot od 0 rad do 2π rad a je náhodně generovaná při každém spuštění simulace, viz blok kódů pod tímto odstavcem. Jedná se o funkci ktreá vrací hodnot u double z rozsahu od double min do double max. To zapříčiní, že startovací bod bude pokaždé jinde na kružnici. Tato proměnná je velmi důležitá, jelikož v důsledku bude velmi ovlivňovat pozorované kvalitativní parametry přenosu. Jednotlivé body na trajektorii jsou určeny pomocí kartézské soustavy v 2D prostoru s pomocí hodnot na ose x a ose y. Hodnoty x a y jsou vypočteny podle vzorců 3.1 a 3.2 , kde hodnoty x_0 a y_0 udávají požadovaný střed kružnice v 2D prostoru. Zvolený *Radius* vyjadřuje poloměr kružnice. Pro lepší názornost je zde pod tímto textem uveden obrázek 3.1a, který graficky zobrazuje výše popsáné parametry. Poslední parametr který zde zbývá popsat je rychlost. Taje definována jako rychlost po obvodu kružnice a byla nastavena na 15 m/s.

```
145 double
146 MeshTest::get_random(double min, double max) {
147
148   return min + (max-min)*(double) rand()/RAND_MAX;
149 }
```

$$x\ [m] = x_0 + Radius \cdot \cos(\theta) \tag{3.1}$$

$$y\ [m] = y_0 + Radius \cdot \sin(\theta) \tag{3.2}$$



Obr. 3.1: a) Parametry pro inicializaci počátečního bodu na kružnici. b)Vyobrazeni pohybu po kružnici podle uhlové rychlosti

3.1 Kvalitativní parametry přenosu

Pro výsledné porovnání směrovacích protokolů bylo vytyčeno několik kvalitativních parametrů, které budou sledovány při každém spuštění jednotlivých scénářů. V první řadě se jedná o ztrátovost paketů během přenosu dat. Dále je počítána propustnost sítě během přenosu dat.

Tyto parametry jsou měřeny intervalově jednou za sekundu a poté graficky zobrazeny jako závislost na čase, kde čas je definován od startu do konce simulace. Tato forma byla zvolena jako nejlepší, jelikož poté lze provést teoretický rozbor simulace v čase a pokusit se detekovat příčinu v dané situaci.

Ztrátovost paketů

Je měřena jako poměr mezi ztracenými pakety a ztracenými pakety plus přijatými pakety. Výsledné číslo může nabývat od nuly do jedné. Toto číslo je vynásobeno stem pro získání hodnoty v procentech. Pro lepší přehlednost je vzorec 3.3 uveden pod tímto textem.

$$LostPaketRatio\ [\%] = \frac{Ztracené\ pakety}{Ztracené\ pakety + Přijaté\ pakety} \cdot 100 \tag{3.3}$$

Propusnost sítě

Je měřena jako poměr mezi přijatými bajty, převedenými na bity a zpožděním od zdroje dat k cíli. Výsledné číslo jsou bity za vteřinu. Poté je číslo převedeno na $Mbit/s$. I zde je výše popsány vzorec 3.4 přehledně zobrazen.

$$Propusnost\ [Mbit/s] = \frac{Přiajté\ bajty \cdot 8}{Latence \cdot (1024 \cdot 1024)} \tag{3.4}$$

Průměrné zpoždění paketů

Tento parametr říká za jaké zpoždění měly pakety s síti. Sledovaní tohoto parametru je za pomoci třídy FLow monitor, který generuje přehledný strukturovaný XML soubor (Extensible Markup Language) soubor, který velmi dobře čitelný s pomoci programu NetAnim, který je součásti programu NS-3.

3.1.1 Důvody ztrátovosti dat v prostředí se sdíleným přístupem

Jelikož je jedná o bezdrátový přenos dat přes radiové prostředí může zde vznikat několik nežádaných jevů, které mají za následek ztrátu dat, nebo jejich nedoručení. První z takových situací je:

Skrytý síťový uzel

Problém nastává když dva síťové uzly v radiovém prostředí vzájemně nedetekují vysílací signál. Poté pravděpodobnost kolize přenosu narůstá. Řešení je buď fragmentovat rámce na menší části, nebo aplikovat rezervaci pásma pomocí dvojice zpráv RTS/CTS (REQUEST TO SEND / CLEAR TO SEND). Ovšem v sítí FANET i toto řešení nemusí být účinné, jelikož prvky se pohybují velkou rychlostí a není lze žádný řídící prvek typu přístupového bodu, takže zde existuje mnohonásobně více možností přenosu dat mezi jednotlivými uzly.

Změny topologie

Směrovací protokoly AODV, OLSR a HWMP byly primárně navrženy pro sítě typu MANET, kde se topologie sítě mění velice řídce oproti sítím FANET. S tím i koresponduje dobu, po kterou jsou cesty ve směrovací tabulce považovány za validní. Tento údaj říká jak dlouho budu znát konkretní cestu k cíli a nebudu znova vyžadovat požadavek na obnovu údajů ve směrovací tabulce.

Například u AODV parametr DELETE PERIOD udává jak dlouho muže mít uzel „A“ uložen souseda „B“ jako aktivní další přeskok na cíl „D“, zatímco „B“ má zrušenou trasu na cíl „D“. Ten je dán vztahem ,kde K je konstanta, s doporučeným nastavením na $K = 5$ a tou je násobena maximální hodnota z ACTIVE ROUTE

TIMEOUT (ART), která je standardně nastavena na 3 ms, nebo parametr HELLO INTERVAL (HI), který je ve výchozím nastavení nastaven na 1 ms viz vzorec 3.5. Pokud budeme brát v potaz, že v simulaci se UAV pohybují rychlostí 15 m/s tak za hodnotu $DELETE\_PERIOD$, což je ve výchozím nastavení 15 ms uzel urazí přibližně za tuto dobu kolem $0,2$ m. Ovšem síťové uzly ve FANET sítích se mohou pohybovat až 125 m/s a za tuto dobu uzel urazí 1.875 m. Pokud k tomu připočteme dobu komunikace mezi jednotlivými uzly, které si tuto informaci musejí vyměnit a vzdálenost mezi uzly mohou být stovky metrů, tak tyto údaje pokud je přijmou už mohou být zastaralé a topologie se mohla již několikrát změnit.

Na Obr.3.2 je uveden příklad, který demonstruje změnu topologie v čase. Zdroj dat je uzel A a cíl dat je uzel E. Všechny uzly se pohybují po kruhové trajektorii s poloměrem 40 m a rychlostí 15 m/s. Dosah antény je nastaven na 250 m a v čase t_1 je označen červenou barvou. V dosahu antény je uzel B, tomu jsou přeposlána data, která přijme a přeposílá dále k cíli. Ztrátovost dat není žádná. V čase t_2 je dosah antény vyznačen modrou barvou. V jeho dosahu je jak uzel A, tak uzel C. Uzel C předá informaci, že cíl D má na dosah s jediným přeskokem. Směrovací tabulka uzlu A je aktualizována. Data jsou přeposílána uzlu C napřímo, ten se ovšem během té doby ztratil z dohledu antény uzlu A. Mezitím byla data odeslána. Ta ovšem nemá kdo přijmou. Uzel B je nepřijme jelikož nejsou pro něj určena a data zahodí. To je jeden z mnoha případů kdy dojde ke ztrátě dat.[2][7][9][11]

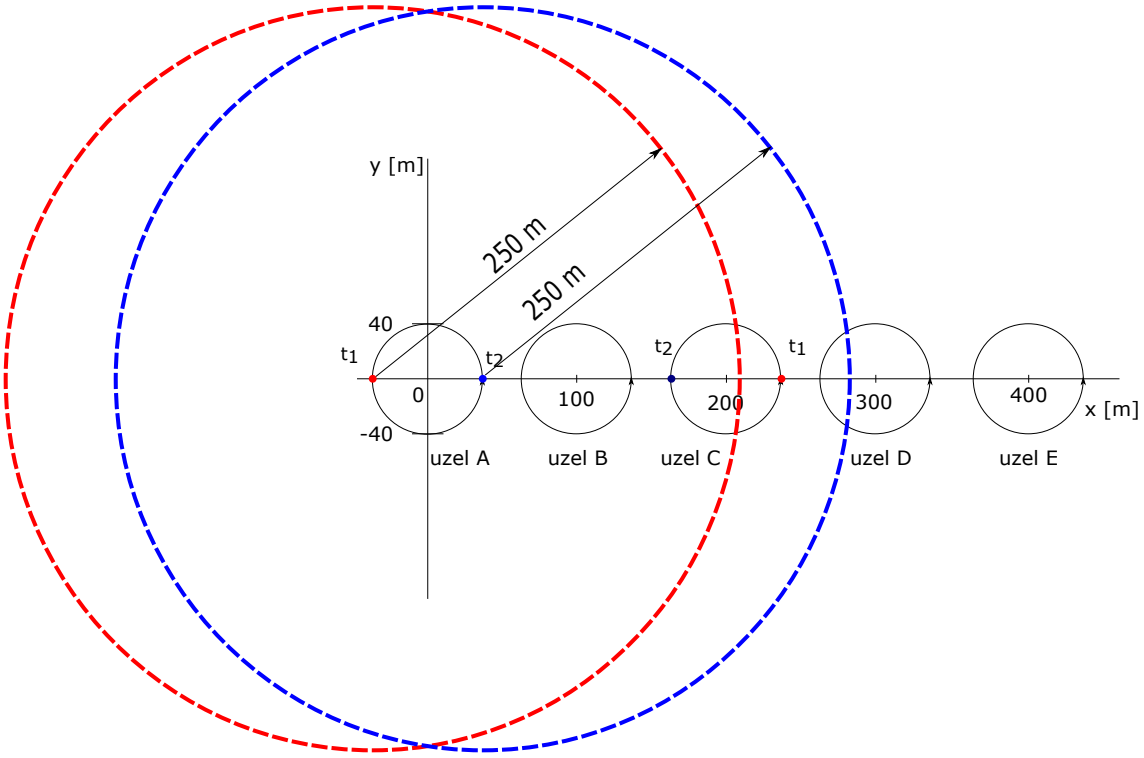
$$DELETE\ PERIOD\ [ms] = K \cdot max(ART, HI) \tag{3.5}$$

3.2 Modely mobility v programu NS-3

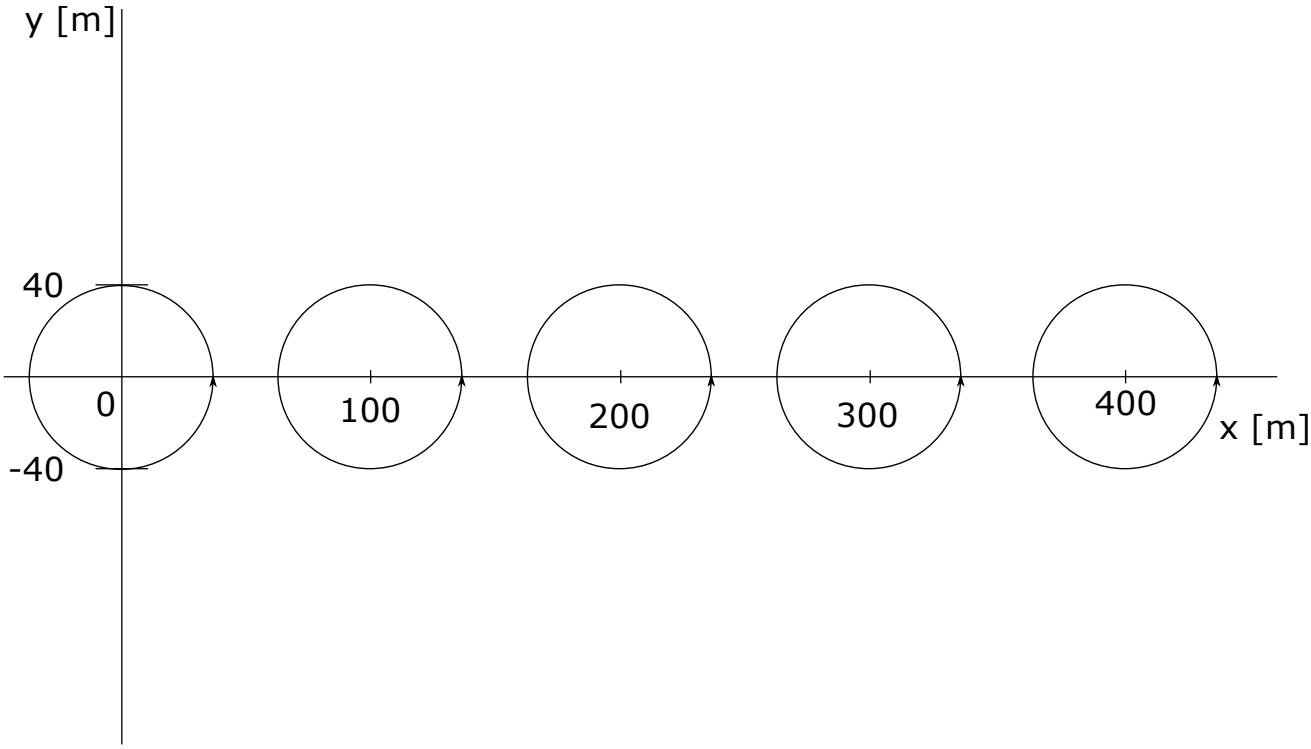
Všechny modely mobility vznikly v programu NS-3, kde je velice dobře zvládnutá problematika mobility síťových prvků a výsledky velmi dobře odráží reálné chování. V rámci diplomové práce vznikly tři modely mobility.

3.2.1 Scénař 1 - Kvazistatický

První scénář se skládá z pěti létajících UAVs, které jsou rozmístěny za sebou s roztečí 100 m a je vyobrazen na Obr.3.3. UAVs se pohybují po kruhové trajektorii s poloměrem 40 m s rychlostí 15 m/s. Jedná se o kvazistatický scénář, kde existuje jen jediná cesta k cíli. UAV umístěný první zleva generuje datagramy UDP, cílem těchto přenášených dat je UAV umístěný první zprava. Jak už bylo zmíněno výše v této kapitole, je vysílací výkon pevně omezen na rádius 250 m, tato vzdálenost byla vybrána záměrně a bude to vysvětleno na demonstrujícím příkladu níže.



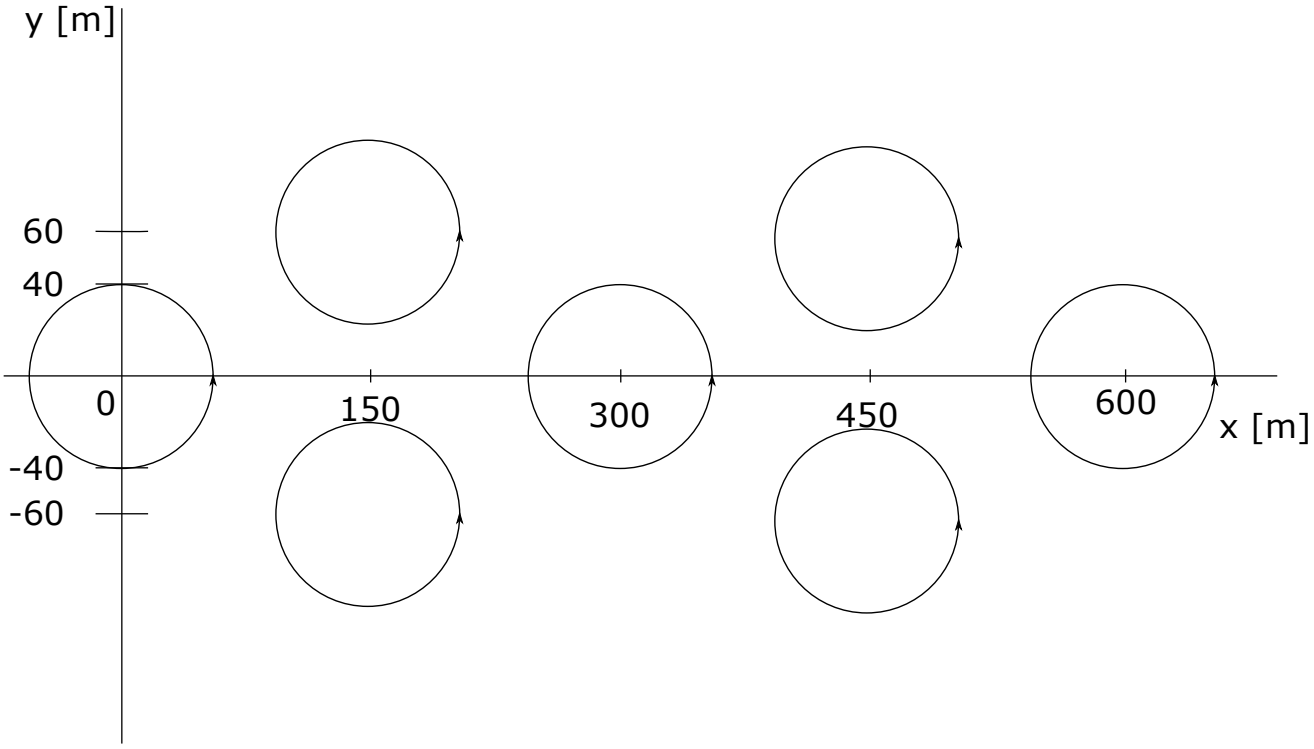
Obr. 3.2: Demonstrace změny topologie sítě.



Obr. 3.3: Scénař první (kvazistatický)

3.2.2 Scénař druhý - Výběr z více tras

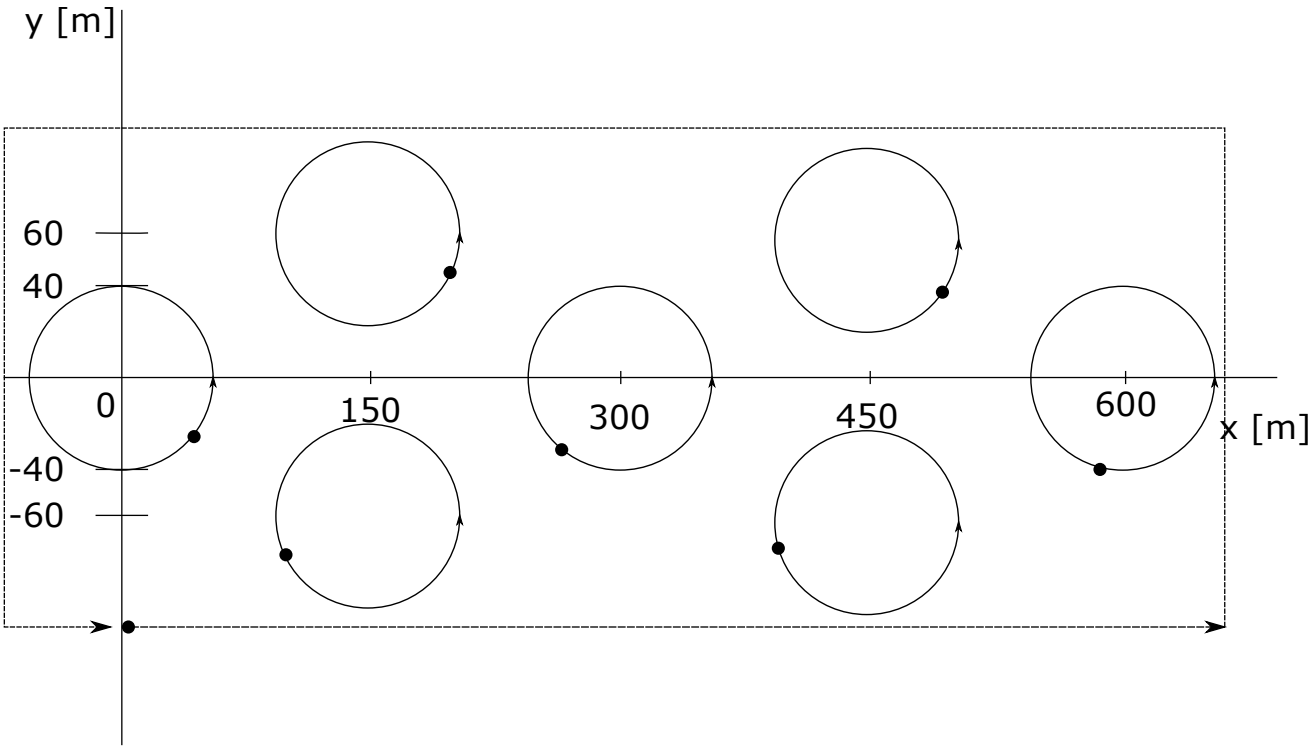
Druhý vytvořený scénář má navíc oproti prvnímu to, že zde existuje možnost výběru z více cest kterou mohou data proudit. Díky tomu se mohou mnohem více projevit rozdíly výsledných sledovaných parametrů při aplikovaní různých směrovacích protokolů. Ovšem ostatní parametry zůstávají stejné jako v prvním scénáři (rádius, rychlost pohybu, zdroj a cíl datového provozu a dosah signálu). Pro lepší názornost je scénář zobrazen na Obr.3.4 a to uzel první zleva.



Obr. 3.4: Scénař druhý - možnost vícecestného směrování

3.2.3 Scénař třetí - Mise

Tento scénář na Obr.3.5 a vychází ze scénáře druhého, ovšem je zde jediná změna. Přibyl zde další UAV, který je zdrojem dat. Tento UAV se nepohybuje po kruhové trajektorii, ale letí rychlostí 15 m/s kolem všech ostatních UAVs a předává data k cíli. Cíl je stejný uzel jak minulém scénáři na Obr.3.4



Obr. 3.5: Scénář mise

3.3 Metodika měření kvalitativních parametrů v programu NS-3

Pro důsledné vyvození závěrů bylo nutné zvolit metodiku jakým způsobem budou jednotlivé směrovací protokoly porovnány. Jelikož, jak už bylo zmíněno v kapitole 3, byl jeden vstupní parametr volen náhodně pro každé spuštění simulace. Jedná se o parametr θ. Ten udává v jakém místě bude startovat uzel na kruhové trajektorii. Tento parametr byl zvolen z důvodu eliminace zvýhodnění počáteční pozice. Ovšem pro relevantní výsledky se musí scénář několikrát opakovat. Počet opakování byl zvolen na hodnotu deset. To dává při třech scénářích a třech protokolech celkové spuštění devadesáti simulací. Udaje jsou sbírány a z těch jsou vytvářeny grafické závislosti ztrátovosti na čase a propustnosti sítě na čase. V grafech nejsou uvedeny všechny průběhy, jelikož výsledný graf by byl nepřehledný. Pro přehlednost jsou zde uvedeny jen některé průběhy, spíše ty zajímavé na kterých lze demonstrovat nedostatky jednotlivých směrovacích protokolů. Dále je zde čárkovanou čarou uveden průměr ze všech deseti průběhů simulace, který bude použit pro celkové zhodnocení směrovacího protokolu u daného scénáře.

3.4 Porovnání směrovacích protokolů v jednotlivých scénářích NS-3

V této kapitole a podkapitolách budou zhodnoceny jednotlivé protokoly v každém scénáři a to ve třech kvalitativních parametrech přenosu sítě. V první řadě ztrátovosti dat, poté propustnosti, která je lineárně závislá na ztrátovosti dat, a posledním parametrem je průměrná doba zpoždění paketů od zdroje k cíli.

Všechny scénáře byly nastaveny tak, aby docházelo k rychlým změnám topologie. Dosah antén jednotlivých uzlů byl zvolen na vzdálenost 250 m proto, aby na jednotlivých uzlech mohly vznikat situace se skrytým síťovým uzlem a omezenou časovou dostupností nepřímých sousedů. Tito nepřímí sousedé rapidně mění směrovací tabulky jednotlivých uzlů, jelikož existuje cesta k cíli, která disponuje lepšími parametry, než disponují přímí sousedé, ale nepřímí sousedé existují v dosahu radiového prostředí jen omezenou dobu a právě tyto situace mohou rozlišovat jednotlivé protokoly podle toho, jak si poradí s touto situací. Výsledné hodnoty sledovaných kvalitativních parametrů jsou proto extrémně nevyhovující a musejí být brány s vědomím, že pro rozlišení směrovacích protokolů musejí být scénáře takto nastaveny.

Ve scénářích je velmi obtížné analyzovat situace proč dochází ke ztrátovosti paketů v daném časovém okamžiku, jelikož ztrátovost je měřena pro celou síť společně. Pro hloubkovější analýzu by se musely samostatně monitorovat všechny možné kombinace uzlů, které v radiovém prostředí dokáží komunikovat mezi sebou. Tím by vznikly desítky měřících dvojic pro jediný scénář, kde by v čase sbíraly informace o lince a vyhodnocovaly ztrátovost a ostatní kvalitativní parametry. Tato metodika je velice pracná a z výsledných informací by bylo určitě lépe patrné proč docházelo k ztrátovosti dat. Ovšem scénáře byly navrhnuty tak, aby ke ztrátovosti docházelo viz kapitola 3.1.1. Není nutné tuto hloubkovou analýzu aplikovat, jelikož důvody proč může docházet k ztrátovosti jsou předem známy.

3.4.1 Porovnání směrovacích protokolů ve kvazistatickém scénáři

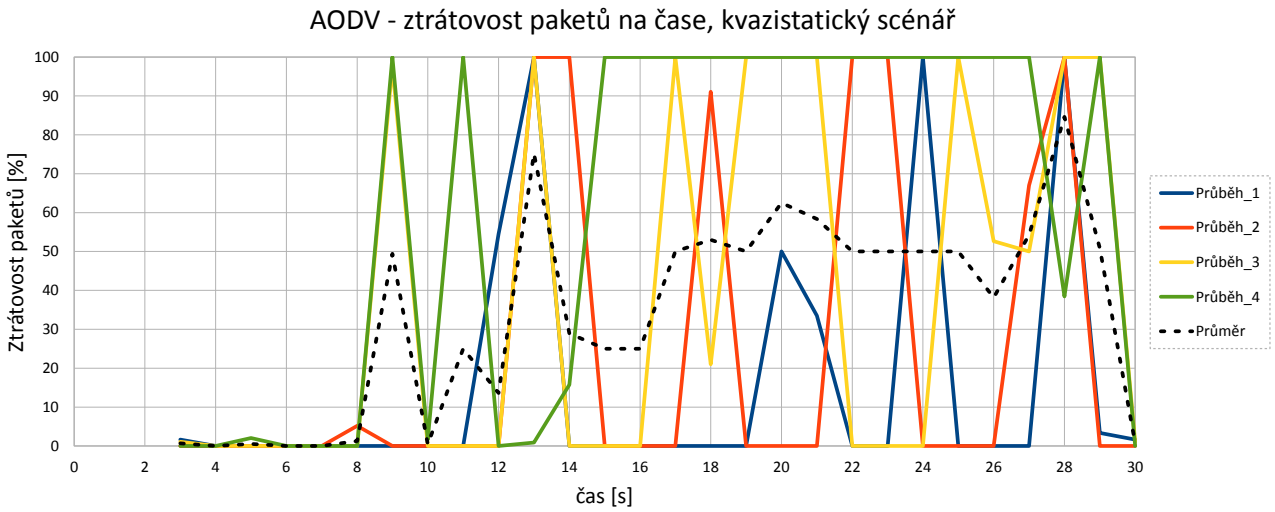
Zde budou rozebrány a porovnány jednotlivé směrovací protokoly podle kvalitativních sledovaných parametrů ve kvazistatickém scénáři, které jsou definovány v kapitole 3.1. Scénář je popsán v kapitole 3.2.1 a rozmístění jednotlivých uzlů popisuje Obr.3.3. Simulace trvala třicet sekund a datový tok byl UDP datagramy s rychlostí odesílaní 2 $Mbit/s$.

Protokol AODV

První na řadě je protokol AODV. Ten si ve kvazistatickém scénáři do osmé sekundy vede velice dobře, ztrátovost paketů osciluje kolem nuly.

Doba za kterou se otočí uzel dokola po kruhové trajektorii je přibližně osmnáct sekund. Po osmi sekundách jde velice dobře vidět, že ve všech průbězích dochází ke ztrátě všech paketů. V tomto čase urazí uzel přibližme sto dvacet metrů, což je skoro půlka obvodu dráhy letu po kruhové trajektorii s poloměrem čtyřiceti metrů. Příčina ztrát dat je pravděpodobně způsobena změnou topologie, ta je popsána v kapitole 3.1.1 a na prezentována na Obr.3.2.

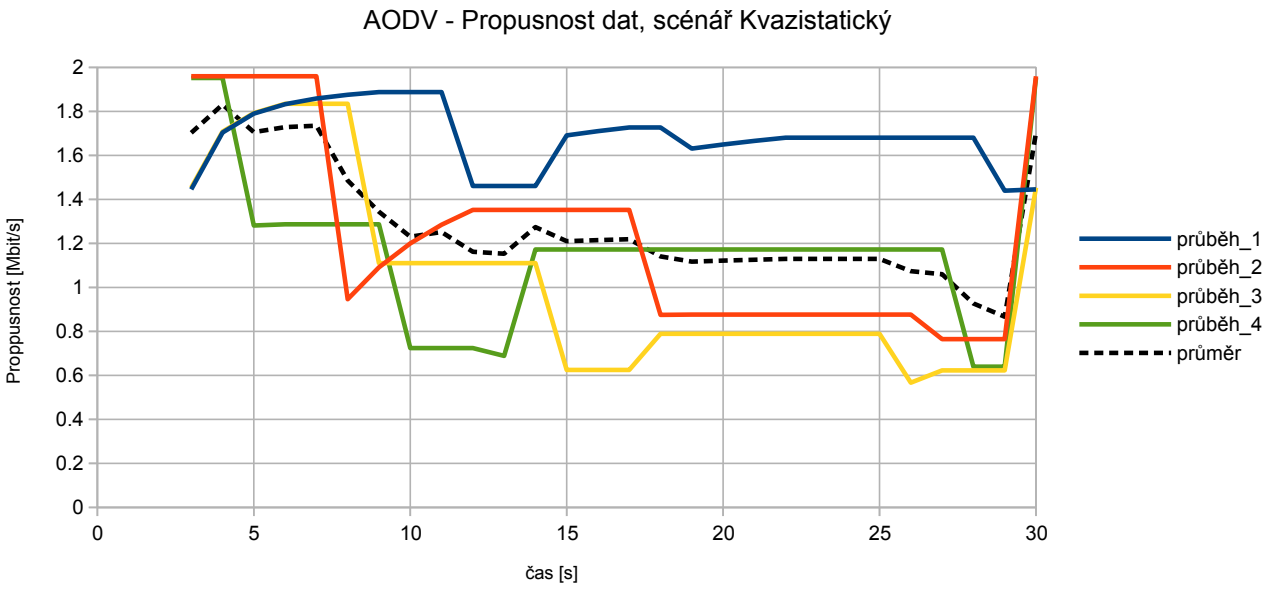
Ovšem protokol AODV je velmi agilní směrovací protokol. Rychlost obnovení linky při ztrátě spojení je průměrně kolem jedné vteřiny viz Obr.3.6. To dokazuje, že reaktivní protokol velmi dobře reaguje na změnu topologie. Propustnost linky v kvazistatickém scénáři se pohybuje kolem $1,3\ Mbit/s$. Průměrné zpoždění paketů v tomto scénáři bylo 450 ms.



Obr. 3.6: Ztrátovost paketů ve kvazistatickém scénáři - Protokol AODV

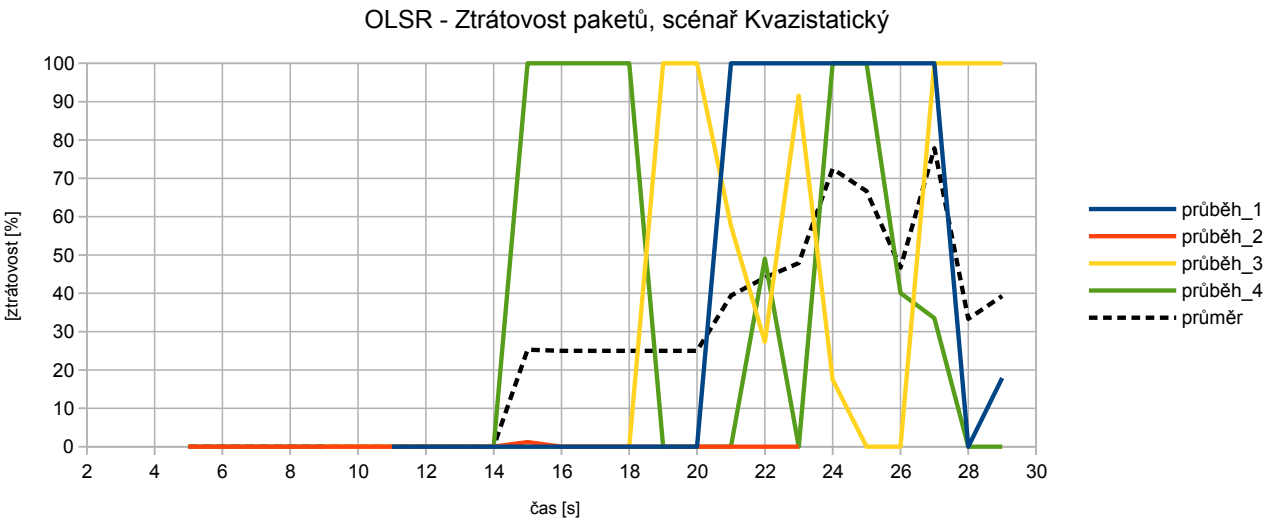
Protokol OLSR

U protokolu OLSR dochází také k velké ztrátovosti dat, což lze vidět na Obr.3.8. Všimněte si v grafu, že přenos dat začal průměrně v čase osm sekund. Do té doby nebyla přenesena žádná data. OLSR protokol je proaktivní protokol a pokud nemá informace o kompletní topologii sítě, nebo alespoň o cíli, kde data budou přenášena, tak data nejsou posílána vůbec. V reálné sítí FANET, kde se může topologie měnit velmi často by nasazení OLSR protokolu bylo fatální a velmi nepraktické pokud by vedla k cíli jediná trasa. Pokud toto pomineme a analyzují se průběhy z grafu tak oproti AODV protokolu při ztrátě spojení je obnova linky pomalejší a pohybuje se



Obr. 3.7: Propusnost sítě ve kvazistatickém scénáři - Protokol AODV

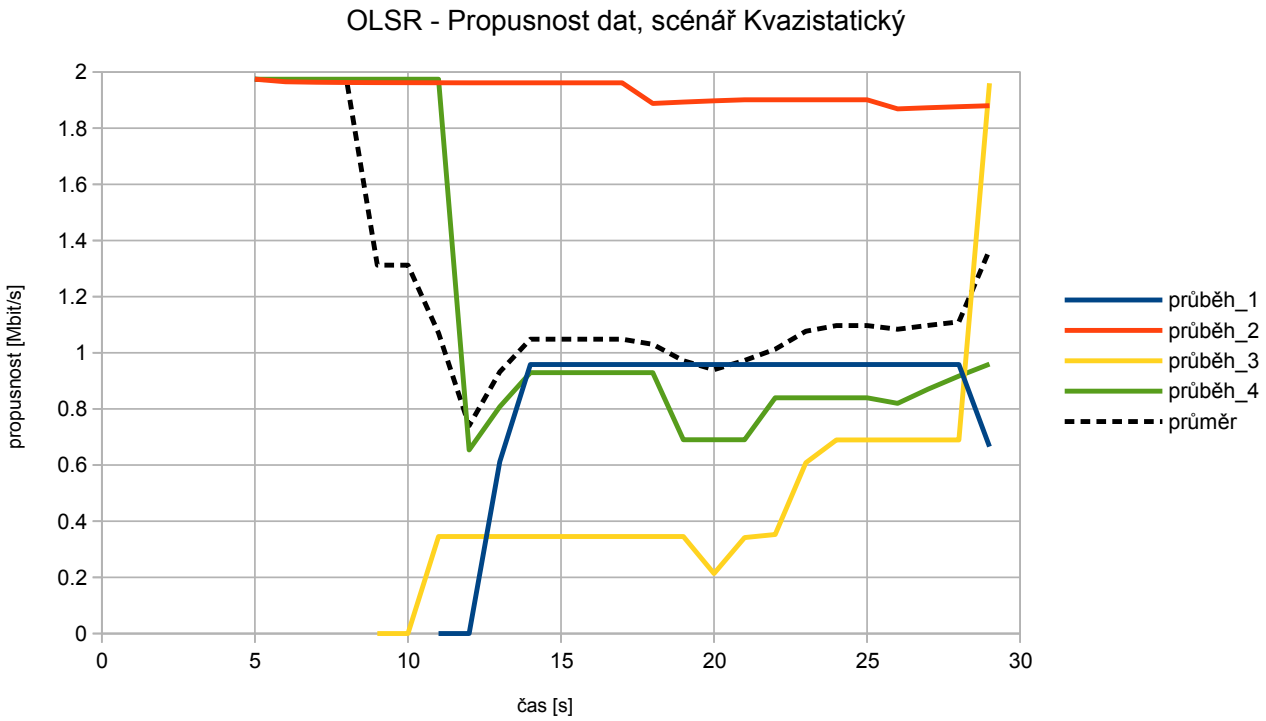
přibližně kolem tří až čtyř sekund. To se odráží i v propustnosti sítě, která průměrně dosahovala kolem 1 $Mbit/s$. Průměrné zpoždění paketů v tomto scénáři bylo 2 sec.



Obr. 3.8: Ztrátovost paketů ve kvazistatickém scénáři - Protokol OLSR

Protokol HWMP

Výsledná ztrátovost z Obr.3.10 a propustnost z Obr.3.11 protokolů HWMP se velice podobá protokolu AODV, kde také dochází ke ztrátovosti dat, ale protokol



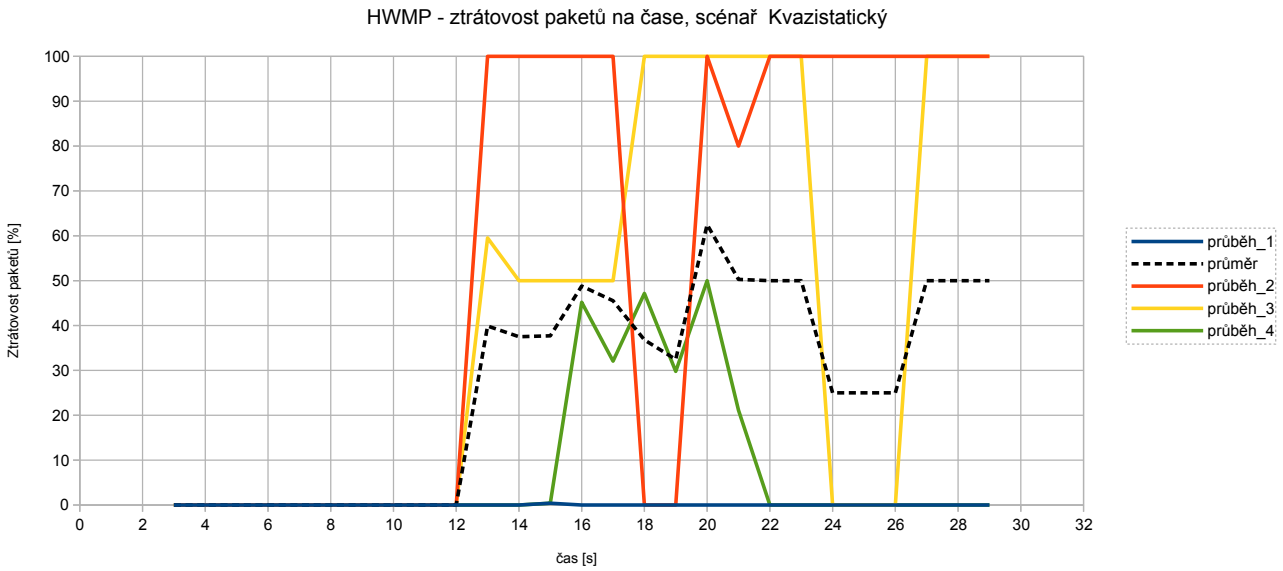
Obr. 3.9: Propusnost sítě ve kvazistatickém scénáři - Protokol OLSR

HWMP při těchto situacích není tak flexibilní a rychlý při obnově linky. Průměrná obnova linky se pohybuje kolem pěti vteřin. Ovšem ztrátovost dat je menší než u AODV protokolu. Do dvanácté sekundy ve všech scénářích nedochází žádné ztrátovosti dat, to je doba kdy všechny uzly urazí vzdálenost 180 m to je přibližné 73 % dráhy po obvodu kruhové trajektorie s poloměrem 40 m. Tuto dobu mohou nastávat situace kdy některý uzel může být dostupný omezený časový úsek, nebo zde dochází k interferencí signálu od skrytého uzlu. Prvním průběhu ztrátovost dat pohyboval pod jedno procento a prostupnost sítě se limitně blížila k 2 $Mbit/s$. U druhého a třetího průběhu od dvanácté sekundy se ztrátovost paketů dosahovala až k 100 %. Průměrné zpoždění paketů v tomto scénáři bylo 850 ms.

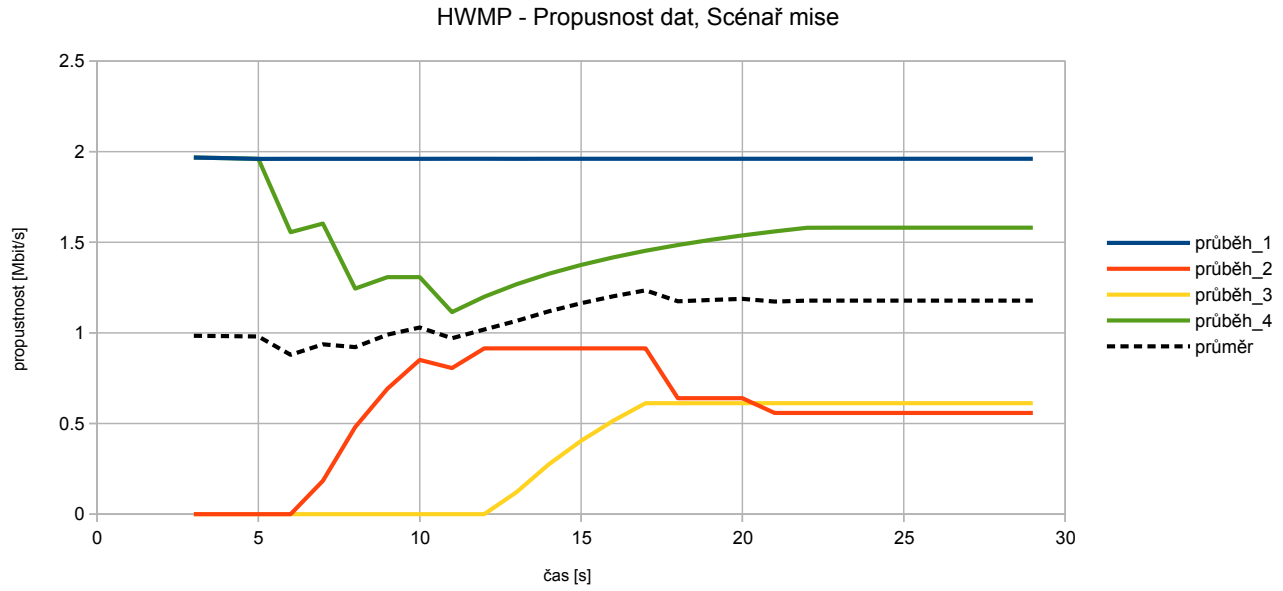
3.4.2 Porovnání směrovacích protokolů ve scénáři „Výběr z více tras“

Protokol AODV

Při nasazení protokolu AODV ve scénáři, kde směrovací protokol může volit z více možných tras k cíli si AODV protokol vedl relativně dobře. V prvním a čtvrtém



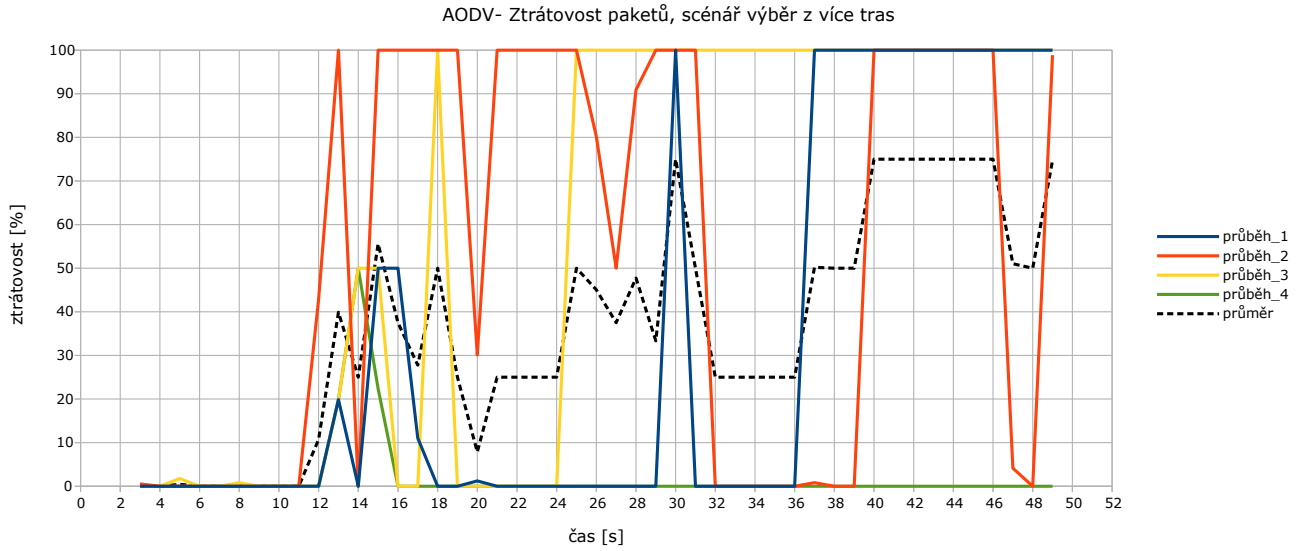
Obr. 3.10: Ztrátovost paketů ve kvazistatickém scénáři - Protokol HWMP



Obr. 3.11: Propusnost sítě ve kvazistatickém scénáři - Protokol HWMP

průběhu simulace lze vidět, že k ztrátovosti dat docházelo poměrně vzácně a když k takové situaci došlo tak protokol AODV rychle obnovil linku v řádu sekundy. To nemůžeme říci o prvním a druhém průběhu simulace. Zde docházelo k ztrátovosti pravděpodobně způsobené častou změnou topologie a tím spojené problémy, které byly popsány již v kvazistatickém scénáři v podkapitole 3.4.1. Průměrná propustnost sítě se pohybovala na úrovni $1,4\ Mbit/s$, což je velice dobrý výsledek s tak

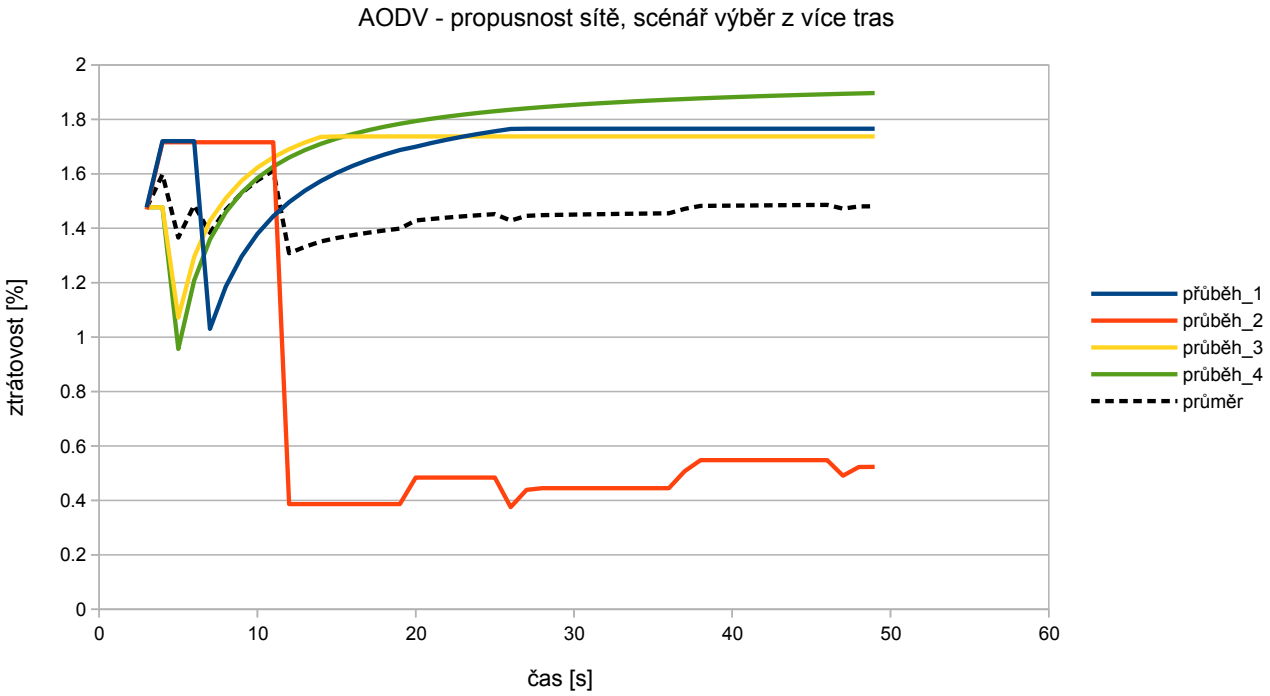
vysokou ztrátovostí dat. Průměrná doba doručení paketu se pohybovala pod čtyři sekundy od zdrojového uzlu k cílovému uzlu. Z toho plyne, že protokol hledá nejkratší možnou cestu k cíli ovšem nezohledňuje následnou ztrátovost dat v síti, jelikož volí uzly podle počtu přeskoků k cíli. Pravděpodobně byly v simulacích ve směrovacích údajích každého uzlu často použity uzly, které figurovaly v radiovém dosahu jen omezenou dobu.



Obr. 3.12: Scénář výběr z více tras - Závislost ztrátovosti paketů na čase pro protokol AODV

Protokol OLSR

OLSR protokol v tomto scénáři si vede velice dobře, což je z Obr.3.14 hned patrné. Ztrátovost byla pod jedno procento ve všech průbězích simulace. Příčina takto dobrého výsledku může být způsobena několika faktory. V kapitole 2.1 jsou popsány charakteristické vlastnosti protokolu OLSR. Stěžejní vlastností protokolu OLSR je to, že uvažuje k nalezení optimální trasy nejen počet přeskoků k cíli, ale bere v potaz i váhové koeficienty jako jsou šířka pásma, zarušení pásma, odstup signálu od šumu a odezvy vytížení sousedního uzlu. A pravě váhový koeficient který monitoruje hodnotu SNR (Signal to Noise Ratio), což je poměr signálu od šumu, může stát za takto výborným výsledkem. Fyzická vrstva v modelu simulace byla experimentálně nastavena, v simulaci byly vytvořeny dva uzly s roztečí mezi sebou na dvě stě padesát metrů. Poté byly upravovány parametry fyzické vrstvy jako jsou vysílací výkony, zisky antén a hodnota detekce odstupu signálu od šumu na obou uzlech při obousměrné komunikaci, aby při této vzdálenosti již vysílací signál nebyl detekován.



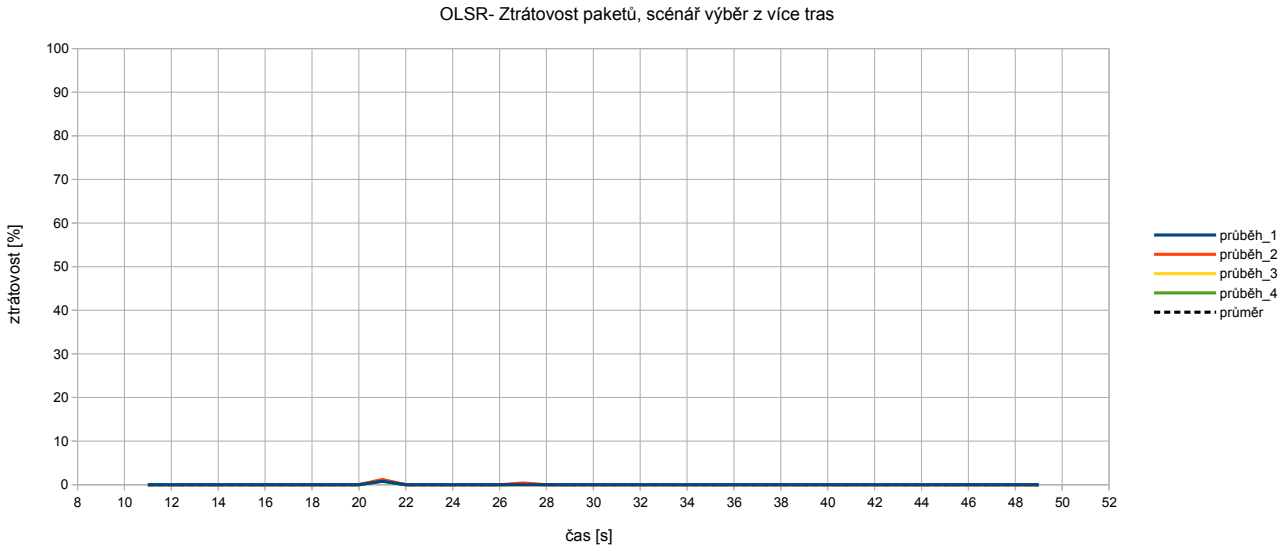
Obr. 3.13: Scénař výběr z více tras - Závislost propusnosti sítě na čase AODV

Váhový koeficient mohl velmi ovlivnit trasu, kterou byly UDP datagramy dopraveny k cíli. Směrovací protokol nemusel využívat všechny uzly, které byly v dosahu radiového spojení, některé jen omezenou dobu viz kapitola 3.1.1. Pravděpodobně byla data posílána pouze ke svým přímým sousedům, nebo směrovací protokol volil alternativní trasy k cíli přes uzly, které nejsou přetěžovány.

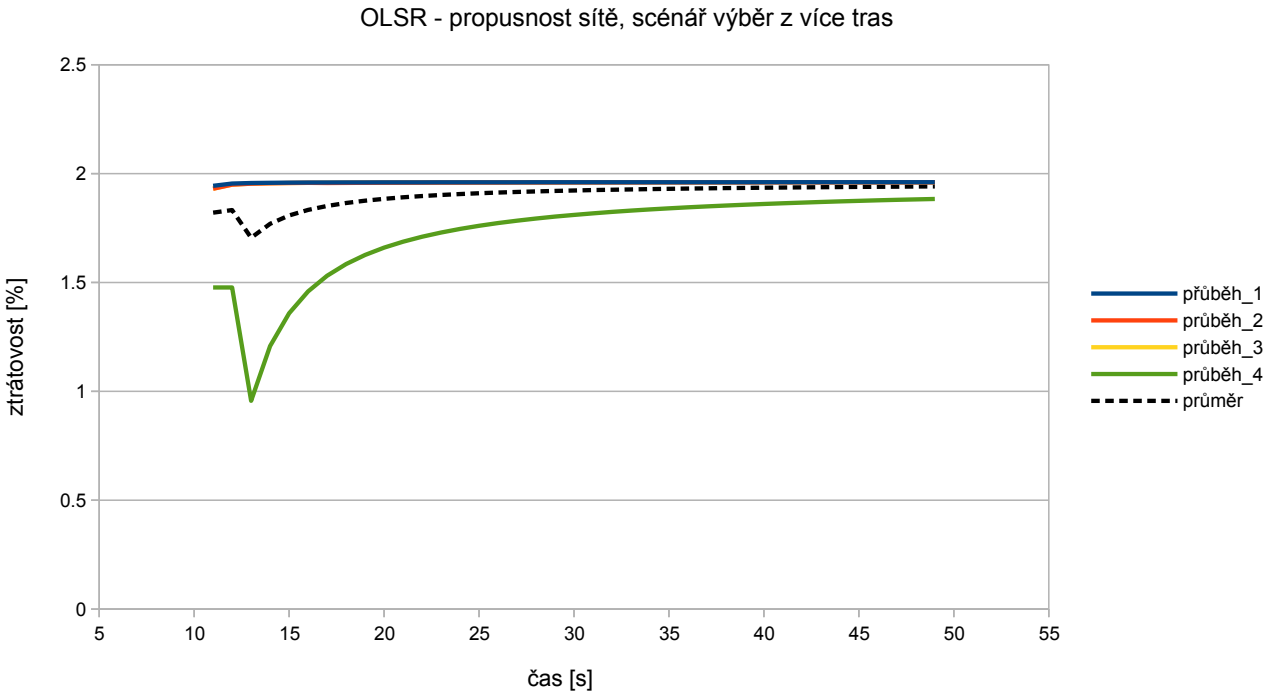
Propustnost sítě z Obr.3.15 při nasazení OLSR protokolu se pohybovala těsně pod hranici 2 $MBit/s$, což koresponduje s ztrátovosti dat, která byla minimální.

Ovšem z Obr.3.14 lze vyčíst, že se opakuje stejný nedostatek jako v kvazistatickém scénáři a to, že data se začala přenášet nejdříve až v jedenácté sekundě simulace i když požadavek na přenos UDP datagramů začal v čase simulace od dvou sekund.

Jak bylo popsáno odstavcích výše k dosažení minimalizace ztrátovosti je muselo někde projevit. Tím nedostatkem byl čas jak dlouho trvalo doručit jednotlivé pakety od zdroje k cíli. Průměrná doba doručení byla jedenáct sekund. Pro aplikace, které pracují v reálném čase je tato doba nevyhovující. V sítích FANET se počítá i s autonomní detekcí kolize mezi jednotlivými UAV. A čas jedenáct vteřin je velmi dlouhá doba. Konkrétněji v tomto případě urazí UAV při rychlostí 15 m/s za jedenáct sekund sto šedesát pět metrů. Musí se brát potaz, že vzdálenost mezi krajními uzly je 600 m, ale i tak tato hodnota je nevyhovující.



Obr. 3.14: Scénář výběr z více tras - Závislost ztrátovosti paketů na čase pro protokol OLSR



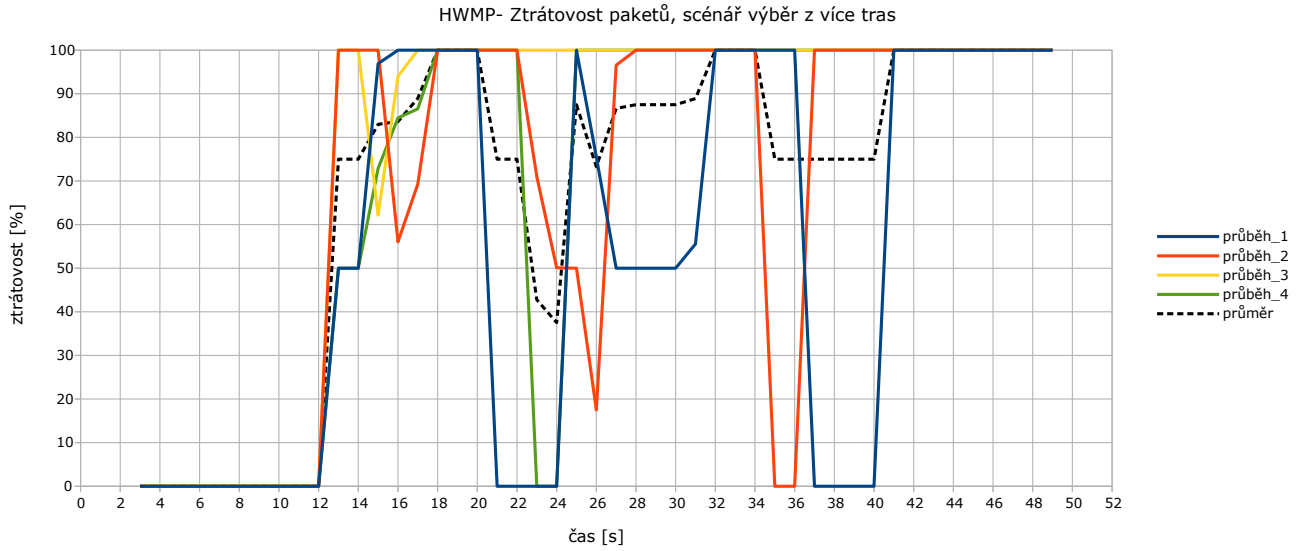
Obr. 3.15: Scénář výběr z více tras - Závislost propusnosti sítě na čase OLSR

Protokol HWMP

U protokolu HWMP se ve scénáři, kde směrovací protokol může vybírat z více možných cest k cíli se HWMP protokolu nedařilo data přenášet. Ztrátovost dat byla ve

všech scénářích enormní a obnova linky při úplné ztrátě dat se nedařila, viz Obr.3.16 zde je vidět podobné chování jako u protokolu AODV, kde také docházelo častým ztrátám dat. Pomalejší obnova cesty k cíli je způsobena proaktivním vyhledávání a znova sestaveni kostry grafu, která se velmi rychle mění v tomto scénáři.

Propustnost v tomto scénáři se pohybovala kolem 0,5 Mbit/s viz Obr.3.17. Průměrné zpoždění paketů bylo

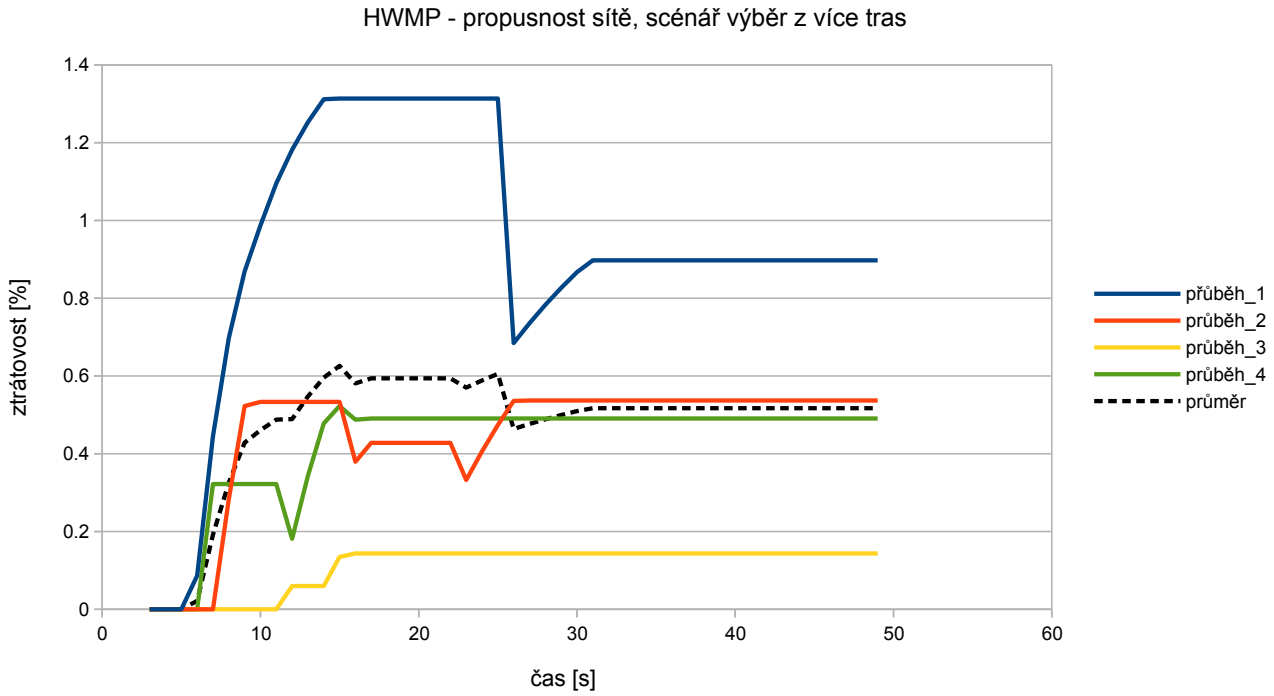


Obr. 3.16: Scénář výběr z více tras - Závislost ztrátovosti paketů na čase pro protokol HWMP

3.4.3 Porovnání směrovacích protokolů ve scénáři „Mise“

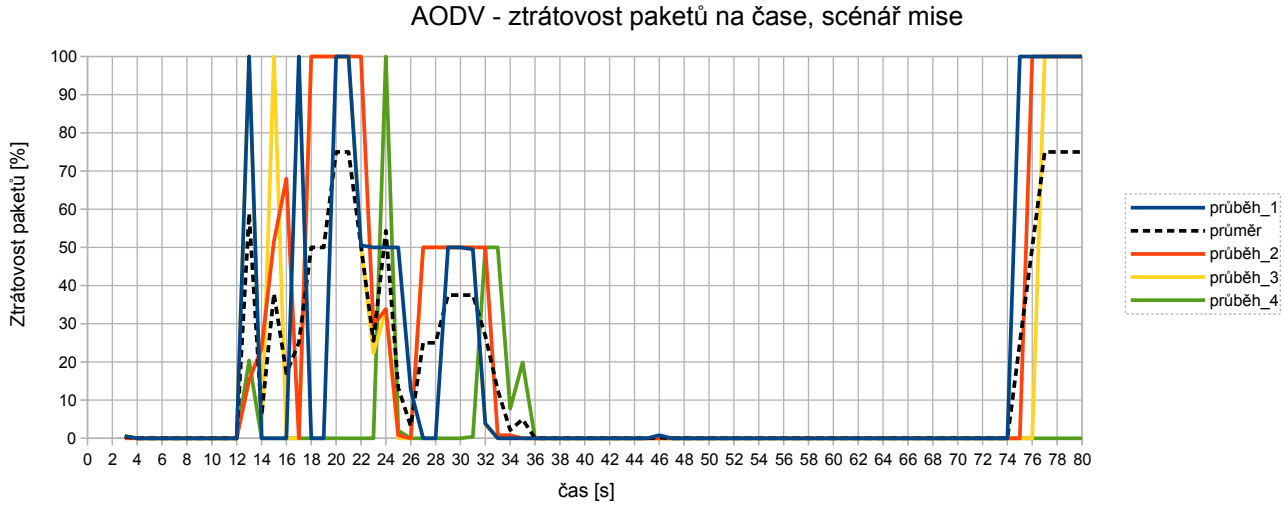
Protokol AODV

AODV protokol ve scénáři mise potvrzuje vlastnost velmi rychle se adaptujícího protokolu, což je patrné z Obr.3.18. Pokud dochází ke ztrátovosti dat, tak ve všech průbězích simulace velmi rychle reaguje na změny topologie a výpadky linky jsou průměrně kole jedné sekundy. Ztrátovost dat do dvanácté sekundy jsou beze ztrát. Za tuto dobu uzly urazily 180 m. Během této doby se topologie pravděpodobně neměnila, jelikož dosah radiového signálu je 250 m a uražená vzdálenost je menší než dosah antény. Do třicáté šesté sekundy docházelo častým výpadkům sítě, kde protokol AODV velmi rychle reagoval na změny. Pravděpodobně pro přenos dat vybíral přímě sousedy a nedocházelo zde častým jevům, které jsou popsány v kapitole 3.1.1. Od této doby ztrátovost dat byla nulová. To je zapříčiněno tím, že vysílací

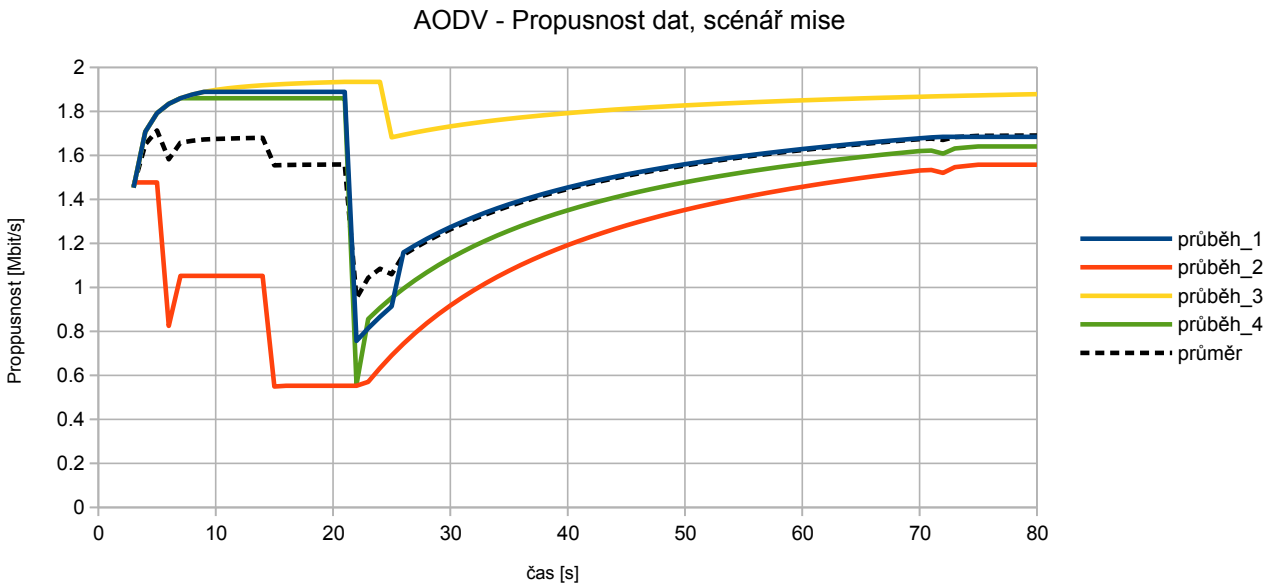


Obr. 3.17: Scénař výběr z více tras - Závislost propusnosti sítě na čase HWMP

uzel má přímou viditelnost na cílový uzel a pro přeposlání dat nepotřeboval jiný uzel. Od sedmdesáti dvou sekund přímá viditelnost na cílový uzel již nebyla možná a údaje ve směrovací tabulce se začala rychle měnit i s topologii sítě. Průměrné zpoždění paketů se pohybovalo kolem $1,5\ ms$. Tato hodnota je ovlivněna scénářem, kde určitý čas byly zdrojové a cílové uzly vedle sebe.



Obr. 3.18: Scénář mise - Závislost ztrátovosti paketů na čase pro protokol AODV



Obr. 3.19: Scénař mise - Závislost propusnosti sítě na čase AODV

Protokol OLSR

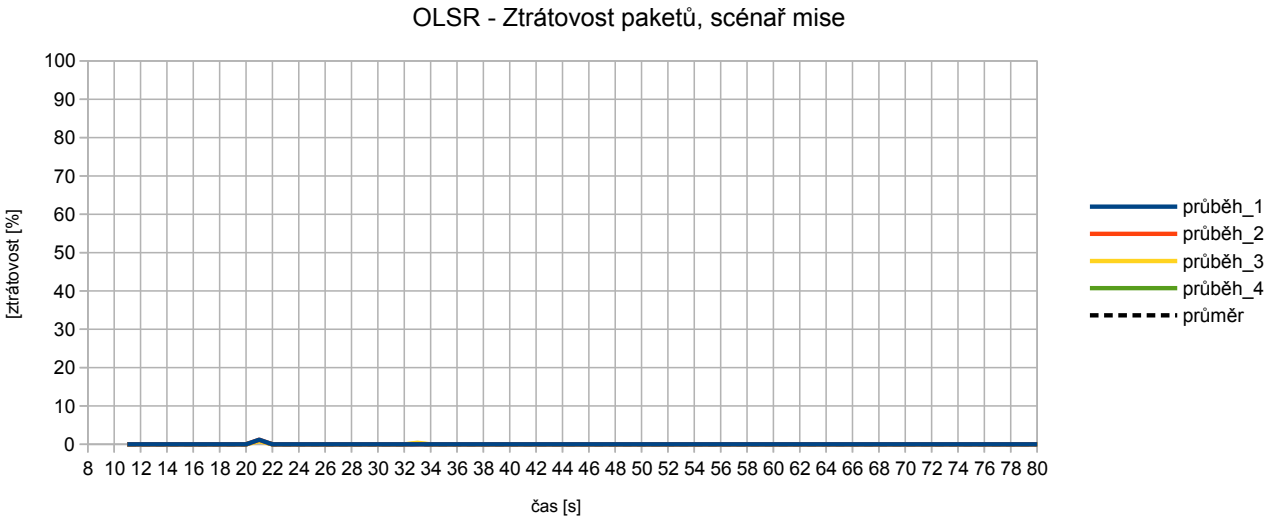
Z popisujícího Obr.3.20 ztrátovosti dat na čase je patrné, že i zde OLSR protokol dosahuje velmi podobných výsledků ztrátovosti dat během simulace jako ve scénáři výběr z více tras, který je popsán v kapitole 3.4.2. Důvody byly stejné jako v minulém scénáři a zde nebudou znova popisovány.

Propustnost sítě atakuje hodnotu 2 $Mbit/s$. Detailněji lze analyzovat propustnost z Obr.3.21. Průměrné zpoždění paketů v tomto scénáři bylo $1,1$ ms.

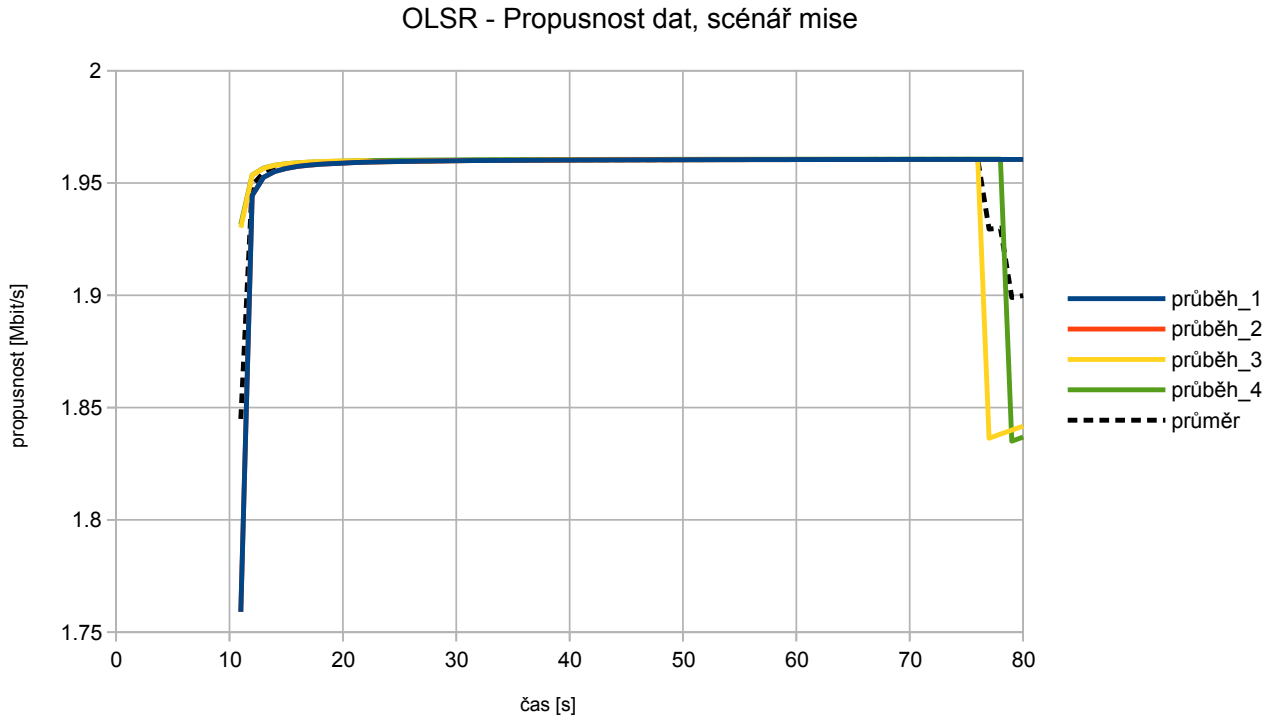
Protokol HWMP

Zde protokolu HWMP svědčilo rozmístění jednotlivých uzlů, jelikož zdroj dat je pohyboval přímočaře kolem ostatních UAV, tím pádem zde nedocházelo častým změnám údajů ve směrovacích tabulkách UAV a ztrátovost se do 34 sekundy pohyboval kolem 35 %. Od 34 sekundy až na jediný případ zde nedocházelo ke ztrátovosti dat, jelikož cílový UAV byl přímý soused zdrojového UAV. OD 62 sekundy cílový UAV již nebyl v dosahu zdrojového UAV a zdrojový uzel musel začít používat k dosažení cíle jiné UAV. Z výsledků plyne, že HWMP protokol dosahuje dobrých parametrů v sítích, kde se topologie nemění často. Jelikož má vyšší režii, hlavně proaktivním modu kde je vytvářena kostra grafu. A nemůže tak rychle reagovat na změny topologie jako protokol AODV.

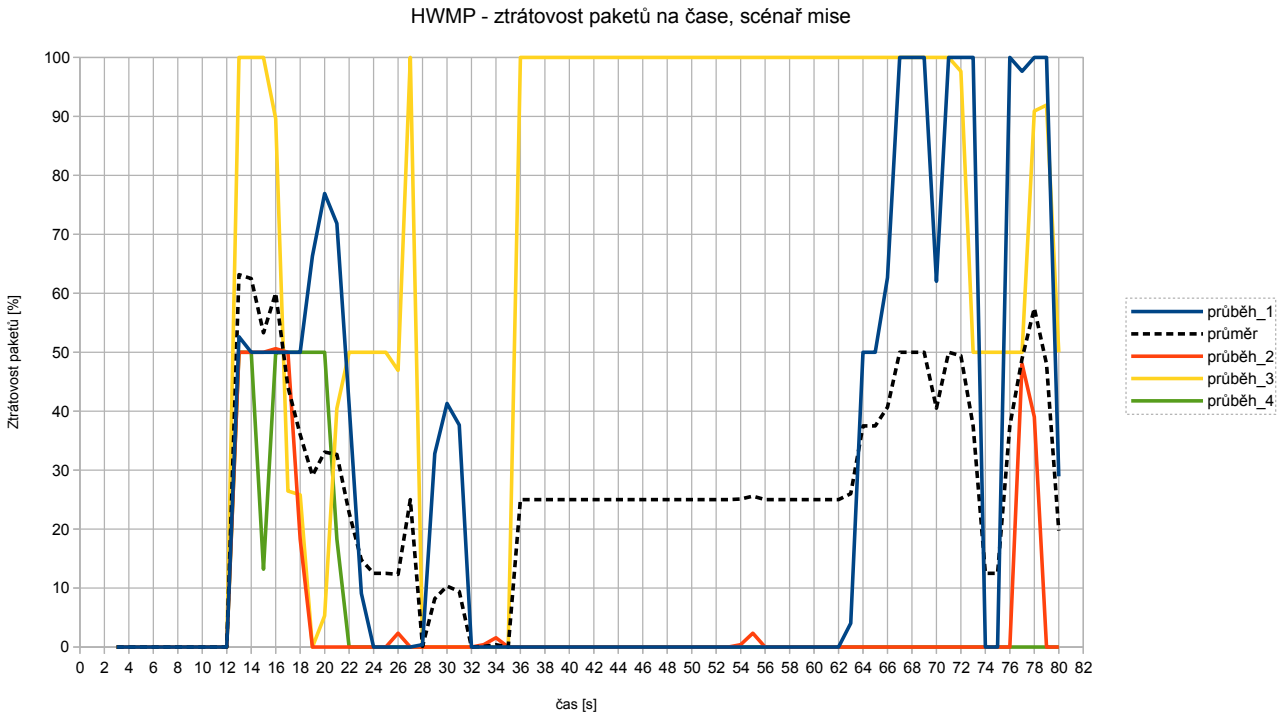
Z Obr.3.23 lze vyčíst, že propustnost průměrně byla kolem 1,5 Mbit/s. Průměrné zpoždění paketů v tomto scénáři bylo $1,4$ ms.



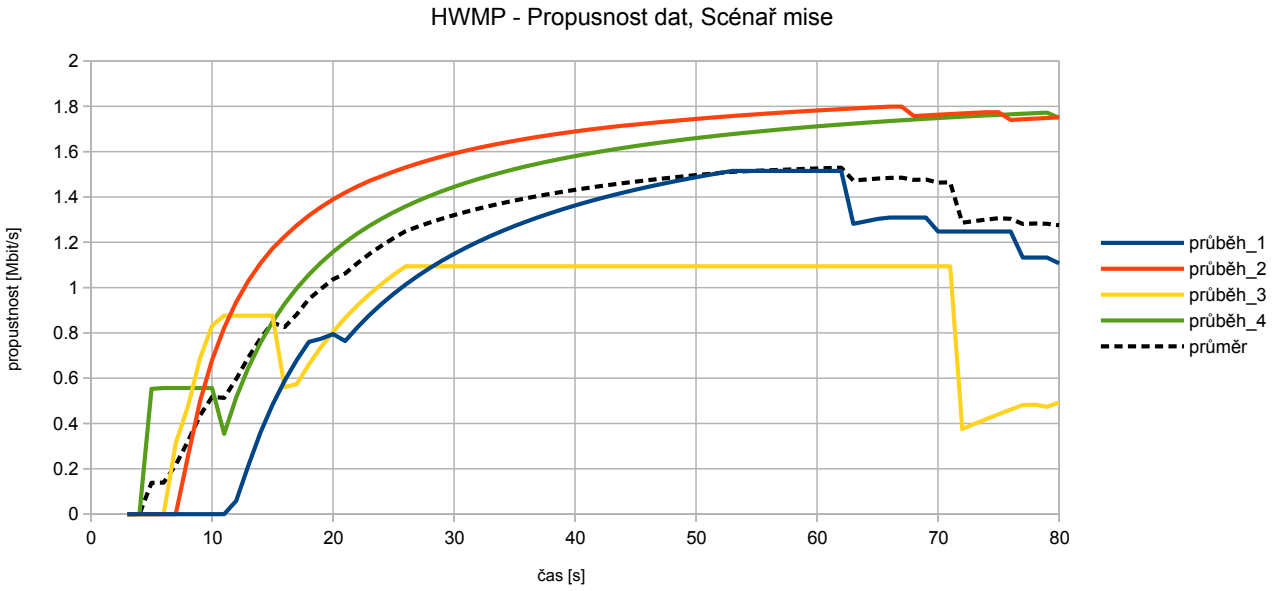
Obr. 3.20: Scénář mise - Závislost ztrátovosti paketů na čase pro protokol OLSR



Obr. 3.21: Scénář mise - Závislost propusnosti sítě na čase OLSR



Obr. 3.22: Scénář mise - Závislost ztrátovosti paketů na čase pro protokol HWMP



Obr. 3.23: Scénář mise - Závislost propusnosti sítě na čase HWMP

4 ZÁVĚR

Cílem této diplomové práce bylo nastínit problematiku směrovacích protokolů, které se využívají v MANET sítích s důrazem na jejich popis, vlastnosti a rozdíly mezi jednotlivými směrovacími protokoly. V prvních kapitolách je rozebrána teorie MANET sítí a poté popsány jednotlivé směrovací protokoly. Ve třetí kapitole jsou popsány vytvořené modely mobility v programu Network Simlator 3, které byly základem pro analýzu směrovacích protokolů, které se využívají v MANET síti a jejich aplikace v sítích FANET.

Vytvořené modely mobility přestavují lítající UAV, které se pohybují vysokou rychlostí po kruhové trajektorii a tyto modely budou sloužit pro porovnání směrovacích protokolů za extrémní hybnosti mobilních uzlů. Na tyto modely mobility byly aplikovány směrovací protokoly, které jsou popsány v kapitole 2. Směrovací protokoly byly porovnány při reprodukovaném proudu UDP dat při konstantní rychlosti přenosu dat 2 $Mbit/s$ na třech scénářích s využitím standartu 802.11n a použití modulace OFDM 54 Mbit/s.

V první řadě se potvrdila očekávání, že směrovací protokoly AODV, OLSR a HWMP nebyly vyvinuty pro nasazení v sítích FANET. Z výsledků lze usoudit, že pro komerční využití by nemohly býti nasazeny, jelikož ztrátovost dat se pohybovala na velmi vysoké úrovni, kdy často docházelo k úplné ztrátě dat a obnova přenosu trvala v extrémních případech až desítky vteřin. Rychlost kterou se pohybovaly síťové uzly v simulacích byla zvolena na 15 m/s, což je velmi malá rychlost v sítích typu FANET, kde uzly mohou dosahovat rychlostí až 125 m/s. V této rychlostí hladině by zcela určitě docházelo k častější změně topologie a pravděpodobnost interferencí signálu a výsledná ztrátovost by byla rapidně větší než naměřené výsledky v této diplomové práci.

Východiskem pro eliminaci všech slabých vlastností již existujících směrovacích protokolů je predikce pohybu okolních uzlů. Jedno z možných řešení problému je například aplikování strojového učení a neuronových sítí a predikovat pohyb ostatních uzlů pomocí umělé inteligence.

Z výsledných grafů v kapitole 3.4 vyplývá, že protokol OLSR si velice dobře vede z pohledu ztrátovosti, ovšem za cenu velkého zpoždění paketu, což limituje tento směrovací protokol pro aplikace, které pracují v reálném čase. Protokol AODV potvrzuje, že dokáže rychle reagovat na změnu topologie a zpoždění paketů bylo třetinové oproti protokolu OLSR. Bohužel AODV protokol nemá žádné jiné mechanismy pro ohodnocení tras k cíli než počet přeskoků. Často využíval uzly, které byly dostupné jen omezenou dobu a pak docházelo ke zbytečným ztrátám paketů. Protokol HWMP dosahoval velice podobných parametrů jako AODV, ovšem větší režie potřebná k sestavení koster sítě způsobovala větší zpoždění paketů než u protokolu AODV. Také

doba, kterou potřeboval HWMP protokol k obnově linky při úplné ztrátě dat byla přibližně o třetinu delší než u AODV. To se projevilo i u propustnosti sítě, která byla menší než u protokolu AODV.

Program NS-3 i v nejnovější verzi 3.26 obsahuje chybu u protokolu AODV. Chyba, nebo špatná definice protokolů způsobuje, že zprávy Route Request jsou rozesílány ostatním uzlům i v době kdy neexistuje žádný požadavek na přenos dat v síti. Vzniká potom otázka zda výsledné hodnoty pro protokol AODV jsou relevantní. Chyba je definována zde [16]

Jak bylo zmíněno výše pro další experimenty, kde by byla implementována predikce pohybu vychází nejlépe AODV protokol, hlavně pro jeho rychlost obnovy linky při přerušení linky a minimální zpoždění doručení paketů a možnost odesílání dat okamžitě po jejich přijetí i když není známa celá topologie sítě.

LITERATURA

[1] RFC 2501, *Mobile Ad hoc Networking (MANET).*[online]. s. 12 [cit. 4.12.2016]. Dostupné z URL: <https://trac.tools.ietf.org/html/rfc2501>.

[2] RFC 3561, *Ad hoc On-Demand Distance Vector (AODV) Routing Protokol).*[online]. s. 37 [cit. 4.12.2016]. Dostupné z URL: <https://www.ietf.org/rfc/rfc3561.txt>.

[3] RFC 3626, *Optimized Link State Routing.*[online]. s. 75 [cit. 4.12.2016]. Dostupné z URL: <https://www.ietf.org/rfc/rfc3626.txt>.

[4] HENNER J.,GRAMES M., *Optimized Link State Routing.*[online]. s. 18 [cit. 4.12.2016]. Dostupné z URL: <http://wh.cs.vsb.cz/sps/images/7/73/OLSR.pdf>.

[5] FARNIK A.,LIŠKA O., PAVELEK P., *AODV routing protokol.*[online]. s. 7 [cit. 4.12.2016]. Dostupné z URL: <http://wh.cs.vsb.cz/sps/images/2/28/AODV.pdf>.

[6] IEEE 802.11S, *HWMP Specification.*[online]. s. 26 [cit. 4.12.2016]. Dostupné z URL: <https://mentor.ieee.org/802.11/public/06/11-06-1778-01-000s-hwmp-specification.doc>.

[7] MEITIS D., VASILIEV D, ABILOV A., *Simulation of MANETs routing protocols for UAVs*. Proceedings Fourth Forum of Young Researchers. Izhevsk, Publishing House of Kalashnikov ISTU, c2014 , pp. 358-363 ISBN 978-5-7526-0649-6.

[8] NS-3 Tutorial *Getting Started.*[online]. [cit. 4.12.2016]. Dostupné z URL: <https://www.nsnam.org/docs/tutorial/html/getting-started.html>.

[9] KOTON, J, *Moderní síťové technologie.*. Skripta VUT Brno, c2013, 191s.

[10] BURGET, R, *Teoretická informatika.*. Skripta VUT Brno, c2013, 198s.

[11] İlker Bekmezci, Ozgur Koray Sahingoz, Şamil Temel. *Flying Ad-Hoc Networks (FANETs): A survey, Ad Hoc Netw.*[online]. [cit. 4.5.2017]. Dostupné z URL: <http://www.sciencedirect.com/science/article/pii/S1570870512002193>.

[12] Stefano Rosati, Karol Kruzelecki. *Speed-aware routing for UAV ad-hoc networks*[online]. [cit. 4.5.2017]. Dostupné z URL: <http://ieeexplore.ieee.org/document/6825185/>.

[13] Erik Kuiper, Simin Nadjm-Tehrani. *Mobility Models for UAV Group Reconnaissance Applications* [online]. [cit. 4.5.2017]. Dostupné z URL: <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=4124182>.

[14] H.T. Friis. *A simple transmission formula for a radio circuit is derived.* [online]. [cit. 4.5.2017]. Dostupné z URL: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1697062>.

[15] Jun Li, Yifeng Zhou, and Louise Lamont, *Packet Delay in Networked Multi-UAV Systems*. Proc. of the 26th International UAV Systems Conference, c2011, Bristol, UK.

[16] NS-3 Bug 1188, *Begin hello transmission only if part of active route* [online]. [cit. 4.5.2017]. Dostupné z URL: <https://www.nsnam.org/bugzilla/show_bug.cgi?id=1188>.

[17] NS-3, *Installation manual* [online]. [cit. 4.5.2017]. Dostupné z URL: <https://www.nsnam.org/wiki/Installation>.

SEZNAM SYMBOLŮ, VELIČIN A ZKRATEK

CTS	Clear to Send
FANET	Flying Ad-HOC Network
GPS	Global Position System
HNA	Host and Network Association
MANET	Mobile Ad-hoc Network
MID	Multiple Interface Declararion
MPR	Multi Point Relays
OSI	Open Systems Interconnection model
RTS	Request to Send
TC	Topology Control
TTL	Time to Live
UAV	Unmanned Aerial Vehicle
UDP	User Datagram Protocol
VANET	Vehicular Ad-hoc Network

SEZNAM PŘÍLOH

A OBSAH PŘILOŽENÉHO CD

- Elektronická verze diplomové práce
- Zdrojové kody z programu ns-3 pro verzi 3.26
  - circularway.cc // zdrojový kód pro circularní pohyb
  - circularway.h // hlavičkový soubor pro circularní pohyb
  - ScenarStaticky.cc // kvazistaticky scénář
  - ScenarMultichoice.cc // scénář vícecestným směrováním
  - ScenarMise.cc // scénář mise
  - readme.txt //návod na instalaci dodatečných souboru do ns-3

B NÁVOD INSTALACE PROGRAMU NS3 A IMPLEMENTACE SOUBORU MOBILITY A SCÉNÁŘŮ

Zde se nachází návod na instalaci programu NS3. NS3 je diskretní silumační program, který je navržen pro operační systém LINUX.

Všechny uvedené soubory jsou uloženy na přiloženém CD

1. Instalaci lze provést podle návodu na domovských stránkách programu NS-3. Ten můžete otevřít na adrese [17]
2. Poté do adresáře `ns3/source/ns-3.26/src/mobility/model/` vložíte soubory `circularway.cc a circularway.h`
3. Další krok je přepsat soubor `wscript`, který je umístěn v adresáři `ns3/source/ns-3.26/src/mobility/`
4. V adresaři `ns3/source/ns-3.26/` spustíte termínál kde zadáte `./waf --clean`. Toto je preventivní krok pro vymazaní všech kompilovaných souborů. To zaručí bezproblémovou funkčnost programu NS3. Kompilovaní je velmi časové náročné podle výkonu pracovní stanice cca. $20min$. Pokud je systém virtualizován tak můžete čekat až hodinu.
5. Poslední krok je nahratí scénařu do složky scratch `ns3/source/ns-3.26/scratch/` a spustění simulace je prováděno pomoci příkazu přes termínal `./waf --run 'scratch/Nazev scenare --protokol=1-3'` parametr protokol říká jaký směrovací protokol bude instalován na všechny uzly v simulaci. [1] - AODV, [2] - OLSR, [3] - HWMP